UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

UNITED STATES OF AMERICA,	)	
	)	CASE NO. CR19-00159-RSL
Plaintiff,	)	
	)	Seattle, Washington
v.	)	
	)	June 15, 2022
PAIGE A. THOMPSON,	)	9:07 a.m.
	)	
Defendant.	)	JURY TRIAL, Vol. 7 of 9
	)	

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE ROBERT S. LASNIK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the Plaintiff:

ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101

For the Defendant:

MOHAMMAD ALI HAMOUDI
NANCY TENNEY
Federal Public Defender's Office
1601 5th Avenue, Suite 700
Seattle, WA 98101

BRIAN E. KLEIN
MELISSA A. MEISTER
Waymaker LLP
515 S Flower Street, Suite 3500
Los Angeles, CA 90071

Reported by:

Nancy L. Bauer, CRR, RPR
Marci Chatelain, CRR, RPR, RMP, CCR
Official Federal Court Reporter
700 Stewart Street, Suite 17205
Seattle, WA 98101
nancy_bauer@wawd.uscourts.gov

INDEX

EXAMINATION OF		PAGE
MATTHEW ORTIZ	DIRECT EXAMINATION BY MR. KLEIN	11
	CROSS-EXAMINATION BY MS. MANCA	14
SETH EDGAR	DIRECT EXAMINATION BY MR. KLEIN	16
	CROSS-EXAMINATION BY MS. CULBERTSON	20
TIM CARSTENS	DIRECT EXAMINATION BY MR. HAMOUDI	26
	CROSS-EXAMINATION BY MS. MANCA	33
ALEX HALDERMAN	DIRECT EXAMINATION BY MR. KLEIN	34
	CROSS-EXAMINATION BY MS. MANCA	76
	REDIRECT EXAMINATION BY MR. KLEIN	95
	REDIRECT EXAMINATION BY MR. KLEIN	101
	RECROSS-EXAMINATION BY MS. MANCA	103
WAYMON HO	DIRECT REBUTTAL EXAMINATION BY MS. MANCA	111
	REBUTTAL CROSS-EXAMINATION BY MR. KLEIN	114
	REDIRECT REBUTTAL EXAMINATION BY MS. MANCA	115

DEFENDANT'S RENEWED MOTION FOR JUDGMENT AND ACQUITTAL BY MR. HAMOUDI 106

GOVERNMENT EXHIBITS

EXHIBIT	ADMITTED	WITHDRAWN
N/A		

DEFENSE EXHIBITS

EXHIBITS	ADMITTED	WITHDRAWN
1203	40	
1204	49	
1207	111	

PROCEEDINGS

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE CLERK: WE ARE RESUMING OUR JURY TRIAL IN THE MATTER OF THE UNITED STATES VERSUS PAIGE THOMPSON, CASE CR19-159, ASSIGNED TO THIS COURT.

THE COURT: THANK YOU.

MR. HAMOUDI, TELL ME WHAT YOU'VE DECIDED.

MR. HAMOUDI: Your Honor, we've decided that we're going to call, this morning, Mr. Edgar, Mr. Ortiz, and Mr. Halderman, and Mr. Carstens, if the court grants the motion, obviously.

THE COURT: And that would be, you said, this morning, but that will be the defense witnesses?

MR. HAMOUDI: That will be the defense witnesses, Your Honor.

THE COURT: And have you discussed with your client, Paige Thompson, the fact she has an absolute right to testify or to not testify, and do you feel she understood those choices?

MR. HAMOUDI: Yes, she does, Your Honor.

THE COURT: And, Ms. Thompson, you've elected not to testify; is that correct?

THE DEFENDANT: Yes, Your Honor.

THE COURT: Do you have any questions about that?

THE DEFENDANT: No, Your Honor.

THE COURT: All right.

So in regard to Mr. Carstens, I will allow him to testify, but I will limit his testimony to reputation, an opinion testimony, not to specific acts that reflect what he's saying.

MR. HAMOUDI: I understand that limitation, Your Honor.

THE COURT: Okay.

Ms. Manca?

MS. MANCA: Your Honor, under 405, the government is allowed to cross-examine about specific instances of conduct related to the reputation.

My understanding is that Mr. Carstens is basing his reputation testimony on a variety of statements Ms. Thompson made, some of which include threats of harm to others, frankly, that he believed to be exaggerated. That was the scope of his representation to the Court.

So I do want to alert the Court that I believe this opens the door to cross-examination on specific instances of conduct that might underlie his opinion about exaggerated conduct.

THE COURT: And you're aware of the specific instances of conduct from what source?

MS. MANCA: Law enforcement reports, social media, those two sources.

MR. HAMOUDI: I'm having a little trouble understanding the substance of what Ms. Manca is talking about,

but I don't intend to ask him about instances or events. I intend to ask him about what he knows of her, based on having known her for about 20 years.

THE COURT: And knowing her reputation in the community in which they live.

MR. HAMOUDI: They live, yes, Your Honor. But I'm unclear about -- he -- I don't -- can I have a second, Your Honor?

THE COURT: Yes.

MR. HAMOUDI: I'll tell you what it is, Your Honor.

In the bond letter, he discusses -- there's a protective order in there and police contacts in Seattle, which the Court is aware of. He's not going to discuss those things. He's not going to -- those are two police matters that involved Ms. Thompson being taken to a hospital. He's not going to get into those matters.

THE COURT: And neither are you, Ms. Manca, right?

MS. MANCA: I'm not going to -- my concern is that, you know, when he says that she's exaggerating, I believe a lot of the exaggeration is going to relate to threats of harm against others that were never carried out. But I'll be very cautious of that, Your Honor.

THE COURT: Yes, please.

Okay. She doesn't have to tip her hand completely on what her cross-examination will be, but I'll be very alert to it.

MR. HAMOUDI: Just so we're clear: If we're going into these two incidents, which was March of 2019, and, I believe, it was sometime later in 2019, it will then require me to put on other types of evidence to explain to the jury that the police officers that were involved in that incident did not place her into custody, but rather saw it as a social health matter and provided her with social assistance.

And so this is why I feel it would go a little bit afield, based on what I'm intending to do with his testimony.

THE COURT: Okay. Thanks.

MR. HAMOUDI: Thank you, Your Honor.

THE COURT: Have we worked out the model AWS contract issue?

MR. HAMOUDI: I'm still waiting on the government, Your Honor.

MS. MANCA: Your Honor, we have reviewed that. I haven't discussed it with the defense yet, but I -- we want the contract to be part of the stipulation rather than the terms that the defense has laid forth.

THE COURT: The sample contract?

MS. MANCA: The sample contract, and we'll stipulate to that as the governing contract, but that's our position.

THE COURT: Yeah, we should do the sample contract.

MR. HAMOUDI: That works for us, Your Honor.

THE COURT: Okay. So get that together.

I did receive, from the government, comments about the jury instructions. One thing I just wanted to raise now -- we're not going to discuss it now -- but the indictment talks about "and" in some places, and the jury instructions use "or" in some places. And there is some case law about deviating from the indictment and, you know, amending by implication.

Will you just look at that and make sure that you want the "or" instead of the "and," will it be appropriate, given the language in the indictment? Okay?

MS. MANCA: Yes.

THE COURT: Great.

And what sequence do you see going forward? Will it be the order that you just gave me in terms of defense witnesses?

MR. KLEIN: Yes, Your Honor. We're going to call Mr. Ortiz first, then Mr. Edgar, then Mr. Carstens, then Professor Halderman.

THE COURT: Okay. Got it.

MR. KLEIN: I think that was the order you received, Your Honor.

THE COURT: It was a little different. It had Edgar first, but thanks for clarifying. That's fine.

And Professor Halderman you've spoken to about -- I mean, he was here -- the understanding of limitations?

MR. KLEIN: I explained that to him, Your Honor, and we don't plan to question him on that. He should not give

answers that would exceed your order.

THE COURT: Okay.

So approximately how long do you anticipate needing? Just the morning, probably, for witnesses?

MR. KLEIN: I think -- I don't know how long the cross of Professor Halderman will go, but I think we will be into Professor Halderman before the lunch break. He may be done before the lunch break.

THE COURT: So right before or after the lunch break, and then we'll take the rest of the afternoon for jury instructions, the motion to dismiss, and any other legal matters, and we'll be ready to move tomorrow morning.

MR. KLEIN: Your Honor, one thing with Professor Halderman, I wanted you to be alerted, we tested out a live demonstration this morning, and he will be doing a live demonstration that is part of a demonstrative exhibit.

THE COURT: Okay.

MR. KLEIN: And I've provided the demonstrative exhibits to the government.

THE COURT: Okay.

Victoria, did we tell jury to be here at 9:15?

THE CLERK: Yes.

THE COURT: Do you want to check and see if we they're there, I'll stay here. We're in recess, so if you need to stand up or move around, go ahead.

(Court in recess 9:15 a.m. to 9:22 a.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Good morning.

We are proceeding with the defense case. Please call your next witness.

MR. KLEIN: Yes, Your Honor. The defense calls Matt Ortiz.

THE COURT: Mr. Ortiz, can you hear us? Do you have a way to get in touch with him?

MR. KLEIN: Yes, we can call him, Your Honor.

THE COURT: Let's try that.

MR. KLEIN: We did test this, Your Honor. It always works on the test.

THE WITNESS: Hello?

THE COURT: Mr. Ortiz, we can hear you, but we're not seeing you.

THE WITNESS: For some reason, the camera icon is grayed out. I cannot turn it on.

THE COURT: How do you want to proceed, Mr. Klein?

MR. KLEIN: I'm happy to proceed with just audio, Your Honor, but I think maybe we could -- there we go.

THE WITNESS: There we go. It took a while.

THE COURT: Yes, and I'm glad you were worth waiting for. Sometimes we get somebody, and we go, "Oh."

I'm Judge Lasnik, and the first thing I'd like you to do is stand and raise your right hand, just like you were in the courtroom, and my clerk will swear you in.

MATTHEW ORTIZ,
having been first duly sworn, testified via Zoom as follows:

THE COURT: The first person questioning you will be Brian Klein for Paige Thompson.

DIRECT EXAMINATION

BY MR. KLEIN:

Q. Good morning, Your Honor.

A. Good morning, sir.

Q. Where do you work?

A. Currently, I'm the chief information security officer for the Ohio Secretary of State's Office.

Q. And where did you work in 2019?

A. I was the cyber operations manager in charge of incident response, as well as other program areas for the cyber security program for the State of Ohio's Governor's Office, with the Department of Administrative Services.

Q. And how long did you work there?

A. I worked there for approximately two and a half years.

Q. So during all of 2019?

A. Correct.

Q. Do you recall being interviewed by the FBI back in August of 2019?

A. Yes, I do recall having conversations with the FBI back in 2019 related to this case.
Q. And do you recall being interviewed more recently by prosecutors and the FBI, just this week?
A. Yes, sir.
Q. And do you recall a cyber incident back in 2019 that was the subject of these interviews?
A. I do, yeah.
Q. And do you recall what type of data was the subject of this incident?
A. Yes, sir, I do. Basically, it was publicly available Ohio crash data that was obtained.
Q. And was that information actually in the possession of the Ohio Department of Administrative Services?
A. It was not. It was actually located -- at the conclusion of the investigation, we determined it was a third party who had, basically, taken data from our publicly available crash feed, and was taken routine by them.
Q. So the data was all publicly available?
A. Correct, yes.
The State of Ohio offers of a service for folks to, basically, either -- for citizens, you can go search -- if you're involved in the crash, you can go to the online crash portal and, basically, search for your crash report, and then for other customers, they provide an automated data feed that

they can, basically, ingest and leverage.

Q. And does that include information, like, names and information in that data?

A. Yeah. Basically, it would be names, addresses, vehicle characteristics, and the circumstances around the vehicle accident.

Q. And did you tell the government that this wasn't actually Ohio's data, it was Phoenix's data?

A. Yes, we did.

During my conversation with the government recently, the name Phoenix Technologies was brought up, and that -- that kind of brought back a lot of these memories of this situation, of all the circumstances.

So we were able to determine, based on the Amazon ID associated with that S3 bucket, that that belonged to a different customer, and that customer was Phoenix Technologies, and it was not a State of Ohio S3 bucket.

Q. And did you also tell the government that the data was all publicly available?

A. Yes, sir.

MR. KLEIN: Nothing further, Your Honor.

THE COURT: Any questions for Mr. Ortiz?

Ms. Manca, Assistant United States Attorney, will ask questions on cross-examination.

CROSS-EXAMINATION

BY MS. MANCA:

Q. Good morning, Mr. Ortiz.

So the data you're talking about wasn't hosted by you when it was taken; is that correct?

A. That is correct.

Q. It was hosted by another company?

A. That is correct.

Q. So your organization was not actually hacked?

A. That is correct.

Q. And the data that the FBI sent you was actually your public information that someone else stored in their S3 bucket; is that right?

A. That is correct.

Q. Okay. And so you don't know the technical details of how that organization was hacked?

A. That is correct.

Q. And the data that the FBI provided you included data that you didn't recognize; is that right?

A. That is correct.

Q. So there was data in that data set that wasn't Ohio DAS data, right?

A. That is correct.

Q. And you don't know whether this organization intended for its data to be public or not?

A. Yeah, I cannot speak to that.
Q. And you don't know whether this other organization wanted this data to be taken or not?
A. I can't speak to that.
Q. And this crash data, does the Ohio Department of Transportation go through some sort of process to decide if this information should be made public?
A. Correct, yeah. So any CPI designed under Ohio law, which is, basically, anything that is for public disclosure, is redacted out of those reports.

So there's, basically, two filed reports; one that, obviously, contains, like, your driver's license number or Social Security number, and the one that's publicly available, basically, has all that data --

Q. Because if you want to make data public, you go through a process of deciding which information should be public, right?
A. Correct.
Q. And you go through a process of deciding how it will be made public, right?
A. That is correct.

MS. MANCA: Okay. No further questions. Thank you, sir.

THE COURT: Anything else, Mr. Klein? Just one moment, Mr. Ortiz.

THE WITNESS: Yes, sir.

MR. KLEIN: Nothing further. Thank you for your time, Mr. Ortiz.

THE COURT: Thank you for your time, Mr. Ortiz.

THE WITNESS: Thank you.

THE COURT: And the defendant's next witness is Mr. Edgar?

MR. KLEIN: Yes, Your Honor.

THE COURT: All right. We'll just take a second for Victoria to bring him in from the room.

Hello. I'm Judge Lasnik, here in Seattle. Thank you, Mr. Edgar. The first thing we're going to do is swear you in, so can I ask you, please, to stand, raise your right hand, and listen to the oath.

SETH EDGAR,
having been first duly sworn, testified via Zoom as follows:

THE COURT: Thank you. Please be seated.

The first questions are going to come from Paige Thompson's attorney, Mr. Klein.

Counsel?

DIRECT EXAMINATION

BY MR. KLEIN:

Q. Hi, Mr. Edgar. Good morning.

A. Good morning.

Q. Where do you work?

A. Currently, I work at a company called AF Group.

THE COURT: Could you repeat the name of the company.

THE WITNESS: Yes. AF Group; alpha, foxtrot, Group.

THE COURT: Thank you.

Q. (By Mr. Klein) And where did you work in 2019?

A. Up until October of 2019, I worked at Michigan State University.

Q. What was your position there?

A. I was their chief information security officer.

Q. And do you recall being contacted by the FBI back in August 2019?

A. Yes, I do; being contacted back, more accurately.

Q. And do you recall they sent you a list of questions about a cyber incident?

A. Yes.

Q. And do you recall talking about the type of data that was at issue?

A. Yes.

Q. And were these email exchanges?

THE COURT: With the FBI?

Q. (By Mr. Klein) With the FBI. Sorry.

A. Yes, with the FBI. I believe there was one or two phone calls in between there as well.

Q. And was part of their inquiry to see what type of data was tied to the cyber incident?

A. Yes.

Q. And what type of data was that?
A. So at the time, Michigan State University had three classifications of data: Public, private, and what we consider confidential and protected information. So this data would have classified as public. The definition of "public data," in this scenario, would be any data that had either been published or released into the public domain by an authorized party, meaning published by the university, published by a researcher, placed in a paper, et cetera.
Q. So the data at issue was, essentially, publicly available data?
A. It was.
Q. And you told the FBI that?
A. Yes.
Q. And were you interviewed more recently by the FBI and prosecutors?
A. Yes.
Q. Just this week?
A. Yes.
Q. And you also were interviewed by an investigator for the Federal Public Defender, too, right?
A. Yes, I was.
Q. And you've given consistent -- you've told all of us the same thing, right?
A. Yes, sir, I certainly hope so.

Q. I've checked. Yes, it's very consistent.
A. Glad to hear.
Q. And so because the data was publicly available, it was, I mean, basically, of no value?
A. I wouldn't say it's of no value. So, for example -- and to be clear, I do not recall the exact data that was in scope for an incident from three years ago. But the data that was -- public data is a very large-umbrella term. It means it can be publicly found. That doesn't necessarily mean that it holds no value.

For example, research data may be -- let's say it's healthcare research data. It may be anonymized data, meaning no patient information is contained therein; however, it could still be immensely valuable data that's released by a research-granting organization, et cetera, where people jockey to get that data, and then publish it as part of their work --

Q. But it's --
A. -- so.
Q. -- publicly --
A. -- it has no value at that point.
Q. But it is publicly available data?
A. Yes, it is publicly available data at that point.

MR. KLEIN: Nothing further, Your Honor.

THE COURT: The Assistant United States Attorney, Ms. Culbertson, will have a couple of questions for you.

THE WITNESS: Great.

CROSS-EXAMINATION

BY MS. CULBERTSON:

Q. Good morning, Mr. Ortiz.

A. "Edgar."

Q. I'm sorry. "Mr. Edgar." That's right. We just spoke with Mr. Ortiz.

Okay. So we just talked about this data being publicly available.

Are you aware of how the data that the FBI sent to you was taken from Michigan State University in this instance?

A. So, first, let me say I'm not going to make a public statement on behalf of a former employer of mine. That seems like it would be a very limiting career move.

However, I will say that my recollection of the events from the investigation we performed was that it utilized overly permissive identity and access management roles on AWS systems that stored the data itself.

Q. Okay. So the data itself was stored in AWS S3 buckets; is that right?

A. I believe so, yes. Unfortunately, I do not have my case notes with me. That would be the property of MSU, right? So, yes, to the best of my recollection, yes.

Q. To the best of your recollection, did MSU intend for the public to be able to access the data in the S3 buckets in the

way that you've just described, and that is via overly permissive permissions?

A. No, I don't believe so.

May I clarify that?

THE COURT: Sure, go ahead.

A. So one of the difficulties of a university is, anybody with a university email account -- and that means an @msu.edu, an @business.msu, @athletics, and so on, can sign up for any services they want, in the name of academic freedom or otherwise. What that leads to is an incredibly broad umbrella of individuals that may place items into any service they go to.

Now, ideally speaking, as an accountable individual, you know, accountable for the security of the organization at the time, the hope is they check in with somebody first. But to register for a free site or a free tool with an email address that has been issued to them is immensely difficult to track down.

So to that point, they vary. To analyze the intent of hundreds of individuals behaving in, hopefully, a secure manner, but not necessarily consulting me first, it became -- it would be very difficult to ascertain all of their intent -- right? -- whether they wanted to make it public through an S3 bucket or not.

What I can say is this -- this appeared to have been a vulnerable configuration of the roles on S3 buckets such that

the data was accessible in, likely, an unintended manner.

Does that make sense?

Q. (By Ms. Culbertson) That does make sense. Thank you for clarifying.

Do you remember using the term "abusing the role" in describing how this data was accessed in this specific case?

A. I do, yes.

Q. Can you explain that to me? What you mean by "abusing the role"?

A. So the way roles work in an identity and access management system, as a whole, is that you define -- hopefully, you define those roles to have the least permission possible.

So if I, as a worker of an organization, don't need administrative capabilities on a system, I shouldn't have them, in general.

If an individual, for whatever reason, was able to and, in this case, did, access that data through -- I won't call it administrative means, but definitely through accessing the back-end storage, not the intended web interface, et cetera, or from an interface, then I would say that either the permissions or the role itself were leveraged in an unintended manner.

Q. Leveraged in an unintended manner.

So is it fair to say that if MSU or somebody within MSU wanted to make this information public, they could do it in a way that would not require accessing it through a role?

A. Yeah, and, more likely, they wouldn't do it this way.
Q. Do you consider accessing this data in this manner, by abusing a role, to be an intrusion?
A. Yes.
Q. And why is that?
A. So regardless of the content of the data for a moment, this is unauthorized access. This is an individual -- and I understand this is public data -- but imagine the attacker doesn't know what they're attacking. Imagine the system was a healthcare system instead, and now they're accessing patient data, or system storing credit card numbers, or a power plant, or a water-treatment plant, or -- the list goes on and on, right?

Legally speaking, I have an obligation to notify unauthorized access to specific types of information.

So had they stumbled upon a different system, I -- I consider this a near miss. Right? This happens to be public data. Thank goodness for me, or for the university in this case.

But overall, had this been another system that was improperly configured or configured in a vulnerable manner, I very well could have been declaring a data breach instead, and notifying the attorneys general all over the U.S., and notifying victims and buying identifying protection services, and all the rest of it. Right?

So the average cost of a data breach, I mean, yes, it's related to a number of records, but, in those cases, that's millions and millions of dollars. I think last year's estimate was, like, $4.8 million.

So we were very fortunate in that this was not -- in those categories of data I gave earlier, this was not confidential data or even private data, which could be maybe shared within the departments of the organization.

Q. Just a few questions about the value of the data. The defense asked you questions about the value of the data, and I believe you testified that it could have some inherent value because it's research data, but just in terms of it having a market value, perhaps, not --

After receiving information from the FBI -- or after reaching out to the FBI -- it sounds like you may have reached out to them first -- did MSU task security specialists to spend time trying to figure out how this breach happened?

A. Yes. I believe that's contained in the same chain of emails.

Prior to getting information from the FBI, we spent -- I want to say -- about 80 hours' worth of work, and then after the fact, about an additional 40 to comb through the data that we had and to provide meaningful data back to the FBI.

Q. And was that meaningful data provided back to the FBI to help with their investigation of the larger breach of,

potentially, other victims?

A. Yes. Part of being a good citizen, I guess.

Q. Okay.

And do you remember, in that email, whether you talked about, sort of, the hourly value of the work of a security specialist?

A. Yeah, I do.

Q. Okay. And was that -- about $75 an hour was your estimate?

A. Yes, it was.

Q. Okay. So 120 hours times 75 would be about $9,000 worth of work for MSU security specialists?

A. Yeah.

MS. CULBERTSON: Nothing further, Your Honor. Thank you, Mr. Edgar.

THE COURT: Thank you, Ms. Culbertson.

Anything else, counsel?

MR. KLEIN: No, Your Honor. Thank you.

THE COURT: Okay. Thanks very much, Mr. Edgar.

THE WITNESS: Thank you.

THE COURT: Bye now.

I think he is a *Star Wars* fan. What do you think?

MR. KLEIN: A Mandalorian, Your Honor.

THE COURT: All right. Mr. Hamoudi?

MR. HAMOUDI: Let me just go grab my witness, Your Honor.

THE COURT: Mr. Carstens, come up to this open area of the courtroom here. We call it the "well" of the courtroom. Please stop there and raise your right hand, and listen to the oath.

TIM CARSTENS,
having been first duly sworn, testified as follows:

THE CLERK: Please state your name for the record, and spell it for the court reporter.

THE WITNESS: My name is Tim Carstens, C-a-r-s-t-e-n-s.

THE COURT: Thank you, Mr. Carstens. You're free to leave your mask on or take it off, whatever you want, as you testify.

Go ahead, Mr. Hamoudi.

DIRECT EXAMINATION

BY MR. HAMOUDI:

Q. Good morning, Mr. Carstens.

A. Good morning.

Q. Do you know Paige Thompson?

A. I do, yes.

Q. How long have you known her?

A. At this time, I want to say approximately 20 years.

Q. We will talk about that, but first I'd like to talk a bit about your background.

Where did you grow up?

A. I grew up in King County, Washington, just outside Sammamish.

Q. And growing up, did you have an interest in computers?

A. To put it mildly, yes.

Q. And when did that start?

A. My relationship with computing systems began at a very young age. Shortly after my family moved to Washington State, my mother enrolled at the University of Washington graduate school. For this purpose, she needed to write a thesis, and we got our computer -- my parents did. And I remember being a very small child sitting on floor next to her while she was working on that machine developing that thesis.

It became an interest of mine, just like vacuum cleaners and other machines at that age. By eight years old, my father taught me the basics of computer programming on that system. By the time I was 16, I'd written my first publication in computer security. The documentation for a computer library called WinPcap, which, at the time, was authored and maintained by Lawrence Berkeley National Labs, and so on and so forth.

Q. So after that, did your interests continue?

A. Yes, absolutely.

While I was in high school, I got my first job as a software engineer, working at a startup that was founded by a retired project manager for Microsoft. He taught me the basics of the industry.

I attended undergraduate at Seattle University here on Capital Hill, earned a bachelor of science in computer science, as well as a bachelor of science in pure mathematics. During that time, I had a research internship at Boeing Phantom Works, which is what introduced me to problems in the space of national security.

Following that, I had an internship at the National Security Agency in the director's summer program, which they advertise as a prestigious program for promising math students.

Following that, I went to graduate school, and shortly thereafter, I returned to my interest in computing -- sorry -- in graduate school, I studied pure mathematics, algebra, geometry, derived interest from my work in cryptography.

Following graduate school, I returned to Seattle and began work professionally full-time as a computer security consultant for two years. Then I left that job and cofounded a company called Inverse Limit, which I worked at for eight years. We did research and development consulting in information security and high-performance computing, mostly for the Defense Advanced Research Projects Agency, but also for certain clients, you know, in private sector, tech companies, financial institutions, things of that nature.

Q. Do you have a security clearance?

A. Not presently, although during my internship with National Security Agency, they -- I filled out an SF-86. They did a full

background check. I was granted -- it's a high clearance. I forget the rules exactly for what I'm allowed to say about that. We'll just leave it there.

Q. That's okay. That's sufficient. Thank you.

A. They talked to my college girlfriend, kids growing up who lived next door, all that stuff.

Q. And you currently work at RiskO, correct?

A. It's pronounced *Risk Zero*, but, yes.

Q. *Risk Zero*. And you're a principal engineer there?

A. That's correct.

Q. I want to go back to Ms. Thompson. How did you come to know her?

A. Paige and I met online in an Internet Relay Chat channel. I want to say it was either '99 or 2000, give or take.

Q. So approximately how old was she?

A. Going off of memory here -- we don't do birthdays -- but I want to say around 14.

Q. And did Ms. Thompson have a handle or a name on that IRC?

A. At that time, I knew Ms. Thompson as "Zero."

Q. Why Zero, if you have an opinion?

A. If I had to guess, I'd say because it is a particularly cool number.

Q. What type of things did you chat about?

A. Computer programming, interesting things that we had found on the Internet, you know, other chat servers, resources about,

say, the Linux operating system. Really nerdy things.

Q. Did Ms. Thompson seem capable?

A. Absolutely.

Q. What would you say about her potential?

A. I would say that everyone in that group was on an extremely promising path, and most of the people in that group have, in fact, proven that right. Among the people in that clique, I would rank Paige as one of the more capable.

Q. Did you know if Ms. Thompson was in school?

A. We didn't discuss school much.

Q. Did you know if she graduated high school?

A. I don't believe that she did, but I don't think we've ever talk about it specifically.

Q. Did you come to know Ms. Thompson in person at all?

A. Yes. After I got a driver's license. As it happened, we were both in the local area.

Q. And what did you know about her reputation after getting to know her in person?

A. Paige was a lot of fun to hang out with. She can be, I would say, energetic, excited, can be the life of the room, also can be quiet. I don't want to say "meek," but maybe -- maybe shy, something of that sort, small, unpresent. I would say both sides are present.

Q. Was there a time where Ms. Thompson came to have a different handle or name?

A. Yes.
Q. What was that?
A. So I'd known Ms. Thompson as Zero for maybe a year or more, but, at some point, the new name had taken hold, which I don't think she picked it for herself, but the new name became Erratic.
Q. Where did that name come from -- what did that name represent to you?
A. Paige's online persona had a tendency to just sometimes say random, off-the-wall, you know, where did that come from sort of stuff in the chat room. For example, in Internet parlance, we call it "scrolling" or "spamming," there's, like, a name for it, Paige didn't invent this behavior, but the basic premise is there's a wall of text that's scrolling by in real time, and you can type anything you want into there, including, for instance, an entire text drawing of a bird, or you can just pick a film and just copy a long list of quotes and paste it right on it, and it will come scrolling by.

So you could be in the middle of a conversation with people, talking about computers, and then all of a sudden, Erratic is being erratic.
Q. And having known her for 20 years, approximately, do you have any opinion as to this erratic behavior, generally?
A. Attention seeking.
Q. And how would you describe, based on knowing her for 20

years, her reputation to express herself and her needs?

A. So I'd mentioned before that, in my view, Paige Thompson was one of the more capable of our clique, and I also mentioned it is a clique, where a lot of folks prove to the promise of that capability and have gone on to have these tremendously exciting careers.

I sometimes think that Paige was -- it's hard to say, but I sometimes think, though, that Paige wasn't able to enjoy that same adventure, in large part, because of this method of communication, which works, I think, perfectly fine in the context of an online chat channel, but which I think doesn't work as well in other contexts, such as a work relationship or maybe certain types of friendships or other things.

Q. Sorry. I forgot to ask.

In the 20 years that you got to know Paige Thompson, did you get to know anything about her family life?

A. Bits and pieces. I have met Paige's mother, for example, when we were teenagers, but only briefly.

As I mentioned before, when I got a driver's license, Paige lived in the area. I think at the time, Paige was in Bothell, but I might be mistaken. I might be confusing locations. Paige moved around a lot.

But I remember, though, that a pretty typical weekend of activity would be, I'd grab my family's minivan, pick up my friends, we'd roll up to Bothell, you know, quite a long drive

from Issaquah, and pick up Paige.

And I don't think that we ever spent any time at Paige's apartment. And I do remember going in once, and the way that you do when you're a kid, I didn't feel particularly comfortable there. I remember that we skedaddled pretty fast.

MR. HAMOUDI: No further questions, Your Honor.

THE COURT: Thanks, Mr. Hamoudi.

Ms. Manca?

CROSS-EXAMINATION

BY MS. MANCA:

Q. Good morning, Mr. Carstens. You're a longtime friend of Ms. Thompson's?

A. Off and one over the years. We've known each other for a very long time.

Q. You care about her?

A. I do.

Q. And you feel sympathetic toward her?

A. Yes.

MS. MANCA: No further questions. Thank you.

THE COURT: Thanks, Mr. Carstens. I appreciate you coming in. You're excused.

All right. Mr. Klein?

MR. KLEIN: We're ready to call our next witness, Your Honor.

THE COURT: And is that the last defense witness?

MR. KLEIN: Yes, Your Honor.

THE COURT: All right. We're moving fast, aren't we? You can step down, Mr. Carstens.

THE WITNESS: Thank you, Your Honor. Which door should I use?

THE COURT: Oh, you can't get out of that door, not even with your security clearance.

THE WITNESS: Thank you, Your Honor.

THE COURT: Okay. Your next witness, Mr. Klein?

MR. KLEIN: Yes, Your Honor. The defense calls Professor Alex Halderman.

THE COURT: Professor Halderman, come on up and raise your right hand to be sworn.

ALEX HALDERMAN,
having been first duly sworn, testified as follows:

THE CLERK: Please state your name for the record, and spell it for the court reporter.

THE WITNESS: My name is Alex Halderman, H-a-l-d-e-r-m-a-n.

Mr. Klein?

DIRECT EXAMINATION

BY MR. KLEIN:

Q. Where do you work?

A. I work at the University of Michigan.

Q. And what do you do there?

A. I'm an educator and a scientist. My job title is Professor of Computer Science and Engineering, and I'm also the director of the University Center for Computer Security and Society.
Q. What's your educational background?
A. I went to college at Princeton University; got my bachelor's degree in computer science. I then stayed at Princeton. I have ten years in New Jersey. I got my master's in computer science and then my doctorate in computer science, where I wrote a dissertation on learning computer security failures.
Q. And do you conduct research as part of your work as a professor at the University of Michigan?
A. I do. I'm a working scientist, so I do research on all aspects of computer security. I try to discover vulnerabilities in real systems that people depend on, and try to get them fixed. I also invent and try to build new defensive technologies to try to keep people safe.
Q. How long have you been doing that work?
A. I've been in my role as a professor since 2009.
Q. And you mention keeping people safe. Do you often assist law enforcement?
A. I do. Research that I've done has helped law enforcement identify the perpetrators in at least one very significant case.
I also do work trying to build defensive technologies, and I've started two different companies that are about different

aspects of defense.

Q. Do you still work at those companies?

A. I have a role in one of them; the other, I don't work at day-to-day.

Q. As part of your work as a professor, do you write papers?

A. I do.

Q. Can you give the jury an overview of the type of papers you write?

A. Sure. So I've published probably approaching 90 technical publications of different kinds, generally peer-reviewed research papers about either the discovery of new vulnerabilities or assessing the security of different kinds of defensive systems or about new technologies. My work, in total, I suppose, has probably been cited in going on 14,000 different scientific papers.

Q. Do you also teach classes?

A. I do. It's one of the favorite parts of the job for me. I teach computer security at the undergraduate level to, approximately, 700 students a year, and occasionally I teach graduate computer-security courses as well.

Q. In addition to teaching classes, do you give speeches?

A. I do, I do. I give technical talks, I give invited talks and keynotes frequently. Public testimony, I've testified to Congress twice about different aspects of cyber security.

Q. And have you received awards and honors, thanks to your

work?
A. Yes. I believe five best-paper awards for the most significant research at different venues. I was named a Sloan Research Fellow, a Carnegie Research Fellow. These are highly competitive, I suppose, different kinds of formal fellowships. And, I think two years ago, I received the University of Michigan's President's Award for National and State Leadership.
Q. And in connection with this case, you've been sitting here attending trial these last two weeks?
A. Yes. I've been present for almost all of the testimony.
Q. And you've reviewed the government's exhibits?
A. I have, yes.
Q. What else have you reviewed in connection with your work on this case? At a high level.
A. Yes. I've reviewed documents from discovery. I've reviewed the data that the government collected from Ms. Thompson's devices and computers. I received the data that she is said to have downloaded.
Q. And we've met and talked regularly, the defense team and you?
A. That's right.
Q. And you mentioned you reviewed Ms. Thompson 's devices. Did you look at things, like the scripts, that have been talked about here in the courtroom?
A. Yes.

Q. And the data that was downloaded?
A. Yes, that's right.
Q. So now I'm going to step away from your background for a moment. Thank you for sharing that.
I want to ask you, at a high level, what was the first thing Paige Thompson did here?
A. Sure. Yeah, I'd be happy to talk about that.
I just want to help, if I can, to put everything in terms that people can understand, because I think maybe some of it seems a little alien and frightening when it's shown just as computer code.
But what Paige Thompson did first was she built what I think has been called a proxy scanner, a tool for searching through a range of Internet addresses for computers that were acting as open proxies.
Q. And do you have familiarity with Internet scanning?
A. I do.
So within the computer security research community, I'm proud to say that my students and I were, you might say, pioneers in introducing Internet-wide scanning techniques as a tool for defensive computer security. We built a tool that we called ZMap that is, today, very widely used in security research, which is an Internet-scanning tool similar to what Paige Thompson built herself.
But the ZMap tool is an open-source tool. It's something

that is free for anyone to use, and it's been used and cited now in something like -- something like, I think, 800 peer-reviewed security studies, used it to try to understand vulnerabilities on the Internet and make people safer.

Q. Could Paige have used ZMap instead?

A. Well, yes, I think she could.

If she had read our paper, read our science and understood this tool, she could have used it to accomplish the same thing that her scanning tools did. Probably it would be approximately one command to make ZMap scan, not only AWS but the entire world, for open proxies, and it would have completed in just a few minutes. It is an extremely efficient tool for this kind of purpose.

Q. And do people use ZMap all the time? Professors, researchers?

A. Yes, researchers around the world, companies use it, et cetera.

Q. Do you have any recent examples?

A. Any recent examples? Well, let me see. What is a good recent example?

Q. A local example?

A. A local example? Sure.

So within the context of proxy scanning, there was a research group a few years ago right here at the University of Washington that used ZMap to scan for open proxy servers all

around the world and to write about what they found and the characteristics of these different open proxies.

Q. And now I'd like to show you what the defense has marked as Exhibit 1203.

Do you recognize this?

A. Yes, I do.

Q. Did you prepare this?

A. Yes.

MR. KLEIN: Your Honor, we'd like to offer this and post it to the jury as a demonstrative.

THE COURT: As a demonstrative exhibit?

MS. MANCA: No objection.

THE COURT: It is admitted for demonstrative purposes and can be displayed now.

(Defense Exhibit 1203 admitted.)

Q. (By Mr. Klein) So, Professor Halderman, I'm going to have you walk the jury through this demonstrative exhibit.

Let's start out at a high level.

What is a proxy server?

A. Right. So I want to try to -- I prepared this to try to explain what a proxy server is, specifically an open forward proxy server, because this is what Paige Thompson's scanner was looking for.

So a proxy server, in general, is a server that makes requests on a user's behalf to another server, and returns data.

There are different kinds of proxy servers, though. And, specifically, we've heard a bit about forward and reverse proxies, but these are terms that even people in the field often confuse, unfortunately.

An open forward proxy server, the kind of proxy server that Ms. Thompson's tool was looking for, is a server that's configured to allow any member of the public to request data from other servers that they, the members of the public, specify.

So it's different from a reverse proxy server, it's different from a closed proxy server. But by "open," we mean the proxy server is configured to serve the public at large. It's not locked down or closed with a password.

By "forward proxy," we mean that it's that end user, the member of the public who is telling the proxy server where to go and what data to bring back.

A reverse proxy, which is a term that's also been used in testimony, a reverse proxy works very differently. A reverse proxy is a proxy server where it's the server operator who is saying where the proxy server will go to get the data and then return it to the public.

But that key distinction, a forward proxy, it's that end user, the member of the public who is commanding the server where to go and bring it back.

So what I've illustrated here, the functioning of an open

forward proxy server, I want to just illustrate so people understand what this functionality looks like. So I'm going to use, as an example, my website, alexhalderman.com, where I have a web page that is the list of courses I teach, teaching.html. And here, this is robot you see in the middle, this is an open forward proxy server. So if I set up my web browser to use the open forward proxy server, and that just means I'm going to go into my web browser's settings, and put in the name of the proxy server and say to my web browser, use this proxy server to fetch web pages. Then if I go to my web browser and put in the URL, alexhalderman.com/teaching.html, my web browser will make a connection to the proxy server and ask it, in essence, in computer protocol verbs, proxy server, please, ask alexhalderman.com for the teaching.html page for me.

The proxy server interprets that, and because it's set up as an open forward proxy server, if it's willing, it will go and make this request to my web server at alexhalderman.com and ask that web server to send it the teaching.html web page.

My web server will then return that web page to the proxy server, and the proxy server will return it to the web browser on my computer.

So this is -- it's as simple as that. It's a server that is willing to make requests for any member of the public for data to other web servers that the member of the public is specifying.

Q. And you work with proxy servers all the time?
A. I do.
Q. Do you recall hearing testimony from Waymon Ho with the FBI about a reverse proxy?
A. Yes.
Q. Was he right in describing what happened here as using a reverse proxy?
A. Well, that's not what Paige Thompson's tool was looking for, and it's not how the servers that she found and interacted with were set up.

So as I say, the key distinction is a reverse proxy, it's the server-operator has configured it to go to specific servers and retrieve data. And the user doesn't have to change any setting in their browser. The user doesn't even know, typically, that the reverse proxy is there.

We often call reverse proxies "transparent proxies," because they're invisible to the user. There's nothing that the user needs to see or know about or set up, and the user is not controlling that destination.

But, as I said, oftentimes people -- even technical people in the field get those terms mixed up. I don't fault Agent Ho for, perhaps, being imprecise.

Q. And why were the proxies in this case open?
A. So why were they open? They were open because they were set up to act -- they were configured to act as forward proxies,

and additional steps hadn't been taken to restrict them. Like you can configure -- when you're setting up a proxy server, you can configure it to be restricted to only be used by specific -- by people at specific IP addresses, where you can lock them down with passwords.

But you can tell from the commands that Paige -- that we've seen Paige ran and got success, that none of those things had been done to the proxy servers where her commands succeeded.

Q. And what was the AWS default, or what is the AWS default?

A. Well, the AWS default for EC2 instances, really, the default is that you don't have ports open to them at all. You have to specify a security policy that allows incoming connections at all before commands can get to a server of any kind.

And the software at issue, several of the alleged victims have testified that they were using the Apache web server software, which also, by default, does not function as an open forward proxy. Someone has to change that configuration to allow that.

Q. And was that true back in 2019, based on your review of evidence?

A. Yes. I've used the Apache software for, probably, 20 years, and that's always been true. I've looked back at old manuals, and, you know, the default has been not to function as a forward proxy.

Q. And on this chart here on Exhibit 1203, is the Apache software the software on that robot? And these are my terms.
A. Yes. So the Apache software -- the Apache HTTP server software can function both as a normal web server, that is something you install on an EC2 Instance that will then return web pages that are stored on that instance, or you can just specify -- just change one option in its settings, and it will behave as an open forward proxy server. You can then specify further options to lock it down, if you choose.
Q. Do you recall the testimony of Mr. Pelaggi from Apperian, or Digital.ai?
A. I do.
Q. And what did he say the default configuration of Apache was?
A. He said that the default was to act as -- he mentioned, specifically, the Apache setting that controls whether it behaves as an open forward proxy, and that's the proxy request setting. He said, specifically, the proxy request was on by default. That's mistaken. The documentation, the code is very, very clear, going back many, many years, that the default is that that setting is off. It doesn't perform as an open forward proxy unless someone has configured it to.
Q. So that means someone at Apperian must have configured it to open that proxy?
A. Someone who set up that server, they or someone acting on

their behalf, had to change that setting from the default.
Q. Do you recall Mr. Fisk testifying from Capital One?
A. I do.
Q. And do you recall him testifying about a mod proxy?
A. Yes.
Q. What is a mod proxy? Can you explain that to the jury?
A. Mod proxy is just a piece of Apache HTTP server software. It's the component of that software that provides both forward and reversion proxy capabilities. And that's where this proxy request setting that can be on or off is. That's also where settings for configuring restrictions on your proxy would be, or settings for setting up reverse proxies.
Q. And mod proxy is part of Apache?
A. Yes.
Q. And do you recall testimony from Mr. Chan from Bitglass?
A. I do.
Q. And did he also talk about the Apache program?
A. I believe, yes, he talked about -- he talked about using the Apache HTTP server as well.
Q. And so in this case -- I just want to, sort of, step back for a second -- what Ms. Thompson was doing was looking for open proxies with a script?
A. Open forward proxies, that's right.
Q. And for the alleged victims in the case, they had open proxies.

A. They did.
Q. And do people deliberately run open forward proxies?
A. Yes, some people do.
Q. Why?
A. Well, there are a lot of different reasons you might provide a forward proxy. Within organizations, sometimes people use proxies to filter Internet access; like, if you want to block access to pornographic sites at a library.

Other people provide public open proxies to allow just members of the public to use their computers to circumvent Internet censorship or other kinds of blocking.

My wife does research -- she is also a computer science professor, and she does research about measuring Internet censorship in countries like Iran and China. And one of the techniques that her research group uses for that is to access open proxies that people have set up in other countries, and use them to try to figure out what people there would be blocked from seeing by their governments.

Q. So when you have an open forward proxy, is a password needed?
A. If it's open, then, no.
Q. Any type of authentication needed?
A. Generally, no.
Q. And from what you've seen in evidence, Ms. Thompson never had to guess at a password, use a password, anything like that?

A. So you can see from her proxy scanner tool, you can see from the curl command she executed, she wasn't providing or guessing a password or any other kind of authentication to make use of those proxies.

Q. And let's use Capital One as an example here.

Did Capital One configure its web application firewall to be an open proxy?

A. Yes.

Q. And what was the general rule that Capital One's open forward proxy followed?

A. So you can tell by the fact that Paige Thompson's command to use it succeeded, that it was working in this way, that it was configured so that any member of the public could use it to request data from other serves that they specified.

Q. And the web application firewalls for the alleged victims, did Ms. Thompson exploit a bug or a flaw in the code?

A. No. This is exactly the way that the Apache software is designed to function, if you have that proxy request setting set to "on."

Q. So the web application firewalls worked as they were programmed and configured to perform?

A. That's right.

Q. So now I'm going to talk about step two.

MR. KLEIN: Can we please pull up for, just for Professor Halderman, Exhibit 1204?

A. Yes, I see it.
Q. (By Mr. Klein) Do you recognize this exhibit?
A. Yes. I prepared this.
Q. And --
MR. KLEIN: Your Honor, I'd like to show this to the jury, publish it to the jury.
THE COURT: 1204?
MR. KLEIN: Yes, Your Honor.
THE COURT: 1204 is admitted for demonstrative and can be displayed.
(Defense Exhibit 1204 admitted.)
Q. (By Mr. Klein) So we have more robots.
Can you explain to the jury what this shows?
A. Yes.
So I prepared this to try to maybe give the Court and the jury a clearer understanding of what it was that Paige Thompson did with respect to Capital One, how she worked with the open proxy and two other separate computer systems involved in order to obtain the data that she did.
So there were really three distinct steps to this. You can see from the commands she executed and the log files and so forth.
The first step involved the open forward proxy, and that's this green robot here, the WAF, their web application firewall, which we know is running the Apache server, the mod proxy

module, and that must have had the proxy request setting turned to "on," because it was acting as an open forward proxy.

So the WAF was configured -- since it was configured as an open forward proxy, it allowed members of the public, including Ms. Thompson, to connect to it and to ask it to retrieve data from other servers. That included another server operated by Amazon called the Instance Metadata Server, IMS, which is shown as the yellow robot here.

So the IMS system, this second system, is used by computers you can have Amazon run for you in order to provide data about their operations and resources and credentials that are made available to them.

But by default, the IMS system doesn't really give out any valuable data to anybody, but you can configure it. As a company that uses AWS, you can configure it to provide more, and that's what Capital One did in this instance, is they configured the IMS system so that it would give out certain credentials in response to requests that were coming from the local EC2 instance. That is, in this case, the web application firewall.

So the web application firewall was allowed to ask the IMS for credentials, and any software on the web application firewall was allowed to do that and would receive them.

The web application firewall was also configured to act as an open forward proxy. So anyone in the public could use it to make requests to any other servers, including IMS.

So what Paige did -- and what anyone in the public could have done -- is she had her computer, she set it up to use the WAF as an open forward proxy, as Capital One had configured it to enable, and then she asked the WAF to ask the IMS computer for these credentials that it was configured to make available, upon request -- in response to any request coming from the WAF.

So she used the proxy, told the proxy go ask IMS for these credentials for something called the ISRM-WAF-Role. The IMS dutifully returned those credentials to the WAF as it was configured, and the WAF returned them to Ms. Thompson's computer as it was configured.

Q. Let me ask you a question real quick.

Did IMS distinguish between the WAF and somewhere else?

A. IMS was -- the way that Amazon has designed IMS, only the local EC2 instance is able to directly talk to it. So it doesn't have a name that is -- it doesn't have what's called a global address. It has only a local address. It's like its name is just, Hey, you over there.

But it was configured -- so that it was configured -- it is built by Amazon and programmed by Amazon to return the data that it has in response to any request that is addressed to it from the EC2 instance.

So it doesn't ask for any authentication, there's no password, there's no cryptography. It's just any request to it, it will return the data that it has.

Q. We're talking about Capital One, as an example, but this would apply, more broadly, to the other alleged victims with similar setups?

A. Yes. This is the way IMS is designed to operate.

Q. And I'll use Capital One as an example.

Did Capital One set up its WAF so that anyone using it, like Ms. Thompson, could make requests to any server they wanted, including IMS?

A. That's correct, yes. That's how it was set up, as an open forward proxy.

Q. So that means all Ms. Thompson had to do was ask the WAF to ask for credentials from IMS?

A. That's right, and that's what this is illustrating, the steps one and two.

Q. And did Ms. Thompson exploit a bug or flaw in the code?

A. No. There's no -- there's no bug. There's no bug in the code to the WAF here. There's no bug in the code to IMS. These are how both of those pieces of software are designed to operate.

Q. And is that what you've heard AWS say?

A. That's how it's documented. That's how it still operates today by default.

Q. So in this instance, all the software so far is performing as it was designed and set up to perform?

A. Each of these components is behaving as it is programmed to

do and as it was configured to do.

Q. So now I'm going to talk about that third step on here. Do you see it, your --

A. Yes.

Q. -- your blue robot.

So after Ms. Thompson gets the credentials through these requests, what happens next?

A. Right.

So now at that point, there's a third computer system involved, and this is another service that Amazon Web Services provides called "S3." And you may have -- I remember the government had a colorful demonstrative about this that illustrates it as a children's sandbox bucket or a beach bucket.

S3 is just, basically, a service that stores data. And S3, by default, when you store data in it, there're no what are called roles or credentials that have permission to read that data. But when you put data in S3, one thing that you can configure is you can configure S3 to tell it to make that data readable by anyone who has -- who's in possession of the credentials for a certain role.

Q. Is that what happened here?

A. And that's right.

In the Capital One instance, just as a concrete example, they had certain data that they configured S3 to say that anyone who comes and is holding the ISRM-WAF-Role credentials, you can

return this data in response to their requests.

They could have configured it in other ways. They could have locked it down further or not assign those credentials to that data, but the fact is, they did configure it so that in response to a request that was bearing those credentials, bearing this string of letters and numbers, S3 was programmed to return this data on request.

Q. Did IMS care that Ms. Thompson got these credentials?

A. No. It's just programmed -- if your request is made using these credentials, return the data. That's its rule.

Q. And could any IP address have done this?

A. I believe so. I don't think there was anything special about where Ms. Thompson was coming from when she was speaking with S3.

Q. And did you see evidence that she did retrieve data?

A. I did.

Q. And based on your review of the evidence, could Ms. Thompson have told what it was before it was downloaded?

A. I don't think so. It appears there were file names, but the file names were not particularly descriptive. She'd have to look at the data, really, to understand what it was or if it was important.

Q. And do people sometimes mislabel file names?

A. Oh, yes, definitely.

Q. Or store old data in them?

A. That's right. Or they're just not particularly descriptive. They could be referring to a lot of things.
Q. They could also hold publicly available data?
A. That's right, or, I suppose, test data, or data that was encrypted and not readable.
Q. Okay. And do people sometimes download all the data in an S3 bucket instead of just a portion?
A. The tools that Ms. Thompson was using, the S3 command line API, makes it really, really easy to just download all the files. She could do that just by running a command called "sync" to download them all at once. To do anything less than all of them would be certainly additional work and more complicated.
Q. Okay. So once that data from an S3 bucket comes onto her computer, did she need to decrypt it?
A. I don't believe so.
Q. And so even if it happened to be encrypted in the S3 bucket, would it have been decrypted when it passed over onto her computer?
A. Yes. S3, one of the modes of encryption that it has encrypts the data when it is stored on Amazon servers. But the way Capital One appears to have set that up, basically, tells S3 to automatically decrypt it and return it if there is a request that's bearing these credentials.
Q. Do you recall hearing a lot of testimony about EC2

instances?
A. Yes.
Q. What is -- we have an S3 bucket here. What is an EC2 instance?
A. So an EC2 instance is just a computer that -- it's, essentially, just a computer that Amazon is willing to run for you, that they will let you do whatever you want with it, and that you're paying them for the amount of time that you're using it.
Q. And so in terms of credentials, was Ms. Thompson given credentials to also use EC2 instances?
A. Yes. So in the case of some of the other alleged victims, the credentials that they had set up, instead of authorizing reading data from S3 buckets, authorized the bearer of those credentials to launch new EC2 instances or to -- basically, to ask Amazon for a new computer that then the bearer of those credentials could use for a period of time.
Q. And you saw and heard testimony about Ms. Thompson -- I'm going to use this word because it's the way I understand it -- spinning up new EC2 instances --
A. Yeah.
Q. -- creating new virtual computers.
When she did that, would she have impaired the servers of the existing customers of AWS at all?
A. In general, no, because they're new, separate virtual

computers that are being spun up. They're asking Amazon for a new, different virtual computer from the virtual computers the customer is already using.

Q. So now I'm going to show you what's marked as Government's Exhibit 205. Do you recognize this?

A. Yes, I do.

Q. And what is this?

A. This appears to be, essentially, a log file that Ms. Thompson would have recorded from some operations that she performed on her computers.

Specifically, this is showing how she's using some simple command line tools to make use of Capital One's open forward proxy, talk to the IMS server, retrieve the ISRM-WAF-Role credential, and then, I recall later on in this exhibit, she's executing some command that is listing what S3 buckets are available.

Q. And is this how it would have appeared on her computer screen?

A. No. Really, the formatting here makes it look more suspicious and maybe frightening than it really would have appeared to Ms. Thompson, all of these strange characters at the top, the numbers, and the little person and dinner plate, that wouldn't have been there. Instead, it would have been in color, and it would have been formatted more nicely. So it wouldn't have looked quite this strange.

But also, even that aside, what this really is is a very, very simple command. It's something that Ms. Thompson could have easily -- almost easily have done in a web browser.

And if you're familiar with this command that's at the core of it, which is this curl command that you see, sort of right underneath that spurious number 97 there on the -- I don't know if that's the fourth or fifth line, but the curl command is just something that -- it's a very, very commonly used computer command that tells the computer to make a web request. And you can tell it to make that web request in different ways.

But it's, basically -- in the simple list form, it's like putting a URL into your web browser and hitting "enter." And this is just a way of doing that from the command line that you can configure and automate in different ways.

But curl is on -- I think it ships with every Apple computer. It probably is on most Windows computers, too. It's almost an ubiquitous command.

Q. I'm going to cut back to Exhibit 1204. I want to talk about this third step a little more.

That third step here says "S3 buckets," but it also talks about EC2 instances, the virtual computers?

A. Yes. So for other of the alleged victims, the credentials that they had configured gave access permissions to start EC2 instances or control EC2 instances. So she would have done, essentially, the same thing that's illustrated here, but the

blue robot, instead of representing S3, would represent the control system for EC2 instances, which is another piece of Amazon Web Services.

MR. KLEIN: Your Honor, I have a few more questions. I felt a break coming. I have about three more questions.

THE COURT: Yeah, that's what I was hoping to get to.

MR. KLEIN: I need one, too.

Q. (By Mr. Klein) So for this third step, the EC2 instance or the S3 bucket, did she need a password or to do any other type of authenticating once she had those credentials?

A. No. The only authentication would be did -- was she possessing the credentials that were assigned that access right.

Q. Again, did she exploit a bug or a code flaw?

A. No.

Q. And, again, this performed as it was programmed and configured?

A. The access control system was performing as it was programmed to do, and the credentials were configured to grant that permission.

MR. KLEIN: Your Honor, I think that's it.

THE COURT: Okay. We'll take our morning break now and, then we'll come back with cross-examination.

MR. KLEIN: I have more with him, Your Honor.

THE COURT: Oh, okay. It's a natural break?

MR. KLEIN: This is a natural break in the subject

matters.

THE COURT: Not a problem. We'll continue with direct examination, and do cross-examination after the break. So eleven o'clock, we'll have you back in here. So we are adjourned until 11:00. Please let the jury head out first.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: So approximately how much more, Mr. Klein, 15, 20 minutes or longer?

MR. KLEIN: Yeah, somewhere between 15 and 20 minutes, Your Honor.

THE COURT: And, Ms. Manca, your cross?

MS. MANCA: Half an hour to an hour.

THE COURT: So we're on track. If we go past noon, I'll let it go to the end so we can finish up, and we'll send the jury home early and do jury instructions and legal matters this afternoon.

See you at 11:00.

(Court in recess 10:44 a.m. to 11:03 a.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: We'll continue with the direct examination of Professor Halderman.

Mr. Klein?

MR. KLEIN: Yes, Your Honor.

Can we please pull up Exhibit 1100?

Q. (By Mr. Klein) Professor Halderman, do you believe that note is referring to what happened here with Capital One?

A. Oh, no question whatsoever. It can only be referring to the setup of their open forward proxy.

Q. And why do you say that?

A. Well, because it's unambiguously referring to the IP address of that machine. It's describing it as an open proxy. And it's mentioning, really, what the key issue is that has us here today, which is the fact that IMS was configured so that there were lots of security credentials or important security credentials available through that proxy.

Q. And you see that term "SOCKS" versus forward?

A. Yes.

Q. Do people get those terms mixed up?

A. Well, as we've seen with the forward versus reverse proxy, people, even technical people, often are imprecise about their terminology around proxies.

Precisely, this was an open forward HTTP proxy, as opposed to an open forward SOCKS proxy. But it's -- I don't know, it's kind of like referring to your computer's hard disk. Modern laptops don't usually have hard disks anymore, they have flash memory. But it's an older term for a related technology that people informally use or imprecisely use.

Q. And should Capital One have been able to figure out that

there was an issue here?
A. I think absolutely, they should have been able to figure it out from this description.
Q. Okay. I'm going talk about --
MR. KLEIN: Can you pull that down, please? Thank you.
Q. (By Mr. Klein) Did you hear testimony in this courtroom about responsible disclosure?
A. Yes.
Q. What does that term mean to you?
A. Responsible disclosure is alerting responsible parties about a security problem in an attempt to get it fixed or to protect the public.
Q. And have you had personal experience with responsible disclosure?
A. Yes. Yes, many times I've -- in my science, in my research, I've discovered security problems and worked to get them fixed.
Q. Can you give us some concrete examples?
A. Oh. Some examples, in one study, we discovered vulnerabilities in -- embedded in IoT 2 devices, things like, you know, your home routers and devices like that, but things that were made by more than 60 different companies. And so reported to those companies about the flaws to try to get them to repair them.

Q. And have you ever been scared to do a responsible disclosure?

A. Yes. Yes, I have.

Q. Why?

A. Well, one of the very first papers that I published was one in which the -- I revealed a defect in a company's product. And they reacted by threatening me and my research adviser at Princeton University with a lawsuit. They were just embarrassed.

Sometimes, when you report problems, companies don't want to hear about it. They either don't take it seriously and don't -- don't respond appropriately or they blame the messenger. Like it's easier sometimes when you've made a mistake to blame the researchers who are bringing it to your attention or the public's attention than it is to just take that reputational hit and fix it.

Q. And do those companies sometimes report those people to law enforcement, in your experience?

A. Yes, yes. I've had my -- people in my community have had experience with that, too.

Q. And are there hard-and-fast rules about responsible disclosure?

A. There might be -- there might be norms, but it's really very, very dependent on the details of the situation. And even after having done this for most of my career, you know, each

situation is a little bit different, and you have to think very carefully about what's going on.

Q. And are there disagreements in the profession about what is responsible, what is ethical, in terms of disclosing?

A. I suppose there are disagreements. There's not a hard-and-fast set of rules that makes something absolutely responsible versus not.

Q. And is it legally required to disclose a vulnerability you discover?

A. No.

Q. And in your experience, is it difficult to navigate responsible disclosure, or just trying to report a vulnerability? Let's maybe use that term.

A. Yes. But -- well, both, I would say, can be difficult to navigate, especially for new people, for -- like I have hundreds of students starting out in security every year who work their way through my classes. And for someone who's just starting out, it can be especially hard. Even for researchers who are experienced on our program committees when we're assessing academic work according to our community norms and trying to decide whether other professional researchers have behaved responsibly, it can often be a long debate without a clear answer.

Q. And do companies sometimes react negatively because they're worried about their own legal liability and reputations?

A. Yes.
Q. And is there one -- just one way to make a responsible disclosure or there are lots of ways?
A. No, no. It's -- really, the core is are you acting to try to protect the public and make things more secure in the end.
Q. Okay. I'm going to pull up Exhibit 203.
MR. KIEN: This is an exhibit that's been admitted by the government, Your Honor.
Q. (By Mr. Klein) Do you recall seeing this exhibit while you were sitting here?
A. Yes, I do.
Q. I'm going to focus your attention on the line that's about one-third of the way down, says "Im gonna dox myself."
A. Yes, I see that.
Q. Do you know what doxing is?
A. Well, doxing often refers to publishing information about the identity, or contact information of someone else online, but dox myself -- dox myself clearly has a different meaning.
Q. What do you think it means here?
A. I think it means basically go public and become -- talk to the public about who I am and what I've done.
Q. Thank you.
I'm going to turn now to Exhibit 1205.
We're coming to the close here.
Oh, actually, this is not quite the close, this is the

beginning of the end.

Can you explain to the jury what this exhibit is?

And we can blow up the different sections as you go through for you, so the jury can see.

A. Yes. So I did an experiment on Monday to try to reproduce what Ms. Thompson has done in this portion of the --

MR. KLEIN: Oh, I'm sorry.

THE COURT: Just a second.

1205, is that illustrative purposes?

MR. KLEIN: Yes, Your Honor, sorry, Your Honor, I forgot, it's only for demonstrative purposes.

THE COURT: Okay. I'll admit it for demonstrative purposes and it can be displayed.

MR. KLEIN: I apologize. I forgot to do that.

THE COURT: That's fine. We both missed it. Yeah.

MR. KLEIN: Thank you.

Q. (By Mr. Klein) We'll start over.

A. Yes. So what you can see at the top here is the command that Ms. Thompson ran involving Capital One's open forward proxy, and that she ran in order to obtain the ISRM-WAF-Role credentials.

And I did an experiment on Monday to try to just reproduce a configuration like that using the Apache server on AWS on an EC2 instance, and to test whether Ms. Thompson could have just done exactly the same thing, you know, web browser.

And so what I did was I went to Amazon and asked for a new EC2 instance, which anyone can sign up for an account and do that.

Q. And that's that virtual computer --

A. The virtual computer; that's right.

And then what I did on the EC2 instance, I installed the Apache web server, just the current version of it.

Q. And that's like the alleged victims did here, at least a lot of 'em?

A. That's the software with the mod_proxy module that several of the alleged victims have testified that they were using.

And I changed just two settings in the default settings. I changed it so that it would use Port 443 as Capital One's server did, and I set the Proxy Requests setting to on, that is the setting that enables it to act as a open forward proxy.

So this comes -- these -- what you're zooming into comes later.

Q. Oh. Apologies.

A. I'm just speaking about how I set up the EC2 instance.

Then I assigned a role in IAM, I created a role, I named it the ISRM-WAF-Role, as Capital One had done, and I assigned that role permission to access an S3 bucket, and I assigned that role to the EC2 instance that I had created.

So setting the permissions, it's a simple model of what Capital One's permissions would have looked at.

Q. And then, again, anybody can go on to AWS and do these same things that you did?

A. That's right. That's right.

So now what I can demonstrate having done that is that, first, a command like the curl command that Paige Thompson ran, would run and succeed.

But then, not only that, but using just a normal web browser, we can do the same thing that Paige Thompson's command did in that browser.

So in this exact -- this illustration, going to use the Firefox web browser just for convenience. Firefox is, I guess, the third most popular web browser now, I don't know, it's a normal web browser that a lot of people use.

So from Firefox, just starting from Firefox, a fresh installation, you just go to its settings, and go all the way down, there's a network settings button you click, and then you bring up this step two window that is the connection settings.

And there, if we can zoom in, what someone would need to do is click manual proxy configuration and type in the address of the AWS instance, the web application firewall in this case, and type in 443, and then click "okay."

Q. And after you clicked "okay," what happened?

A. And after you click "okay," you're just in the normal web browser. It's just set up to use this open forward proxy when it makes connections, okay.

And then we can go to step three. And then Ms. Thompson, or really anyone, could type in the IP address of the IMS system.

This is publicly known, and it's in the Amazon documentation, 169.254.169.254. And then her browser would use that open forward proxy to make a request to IMS.

And if you just type in that IP address by itself without the rest of the path, it basically gives you -- it gives you different options.

One of those options is latest. You know, just then take latest, put it onto the end of the path, it gives you several options, one of them is metadata. You put metadata onto the path, et cetera. And so you can navigate in your web browser to this full URL just starting with the IP address of the IMS.

But, anyway, after constructing that full URL that you see in blue at the top, the same one that Ms. Thompson's curl command enters, if you put that into the web browser and hit enter, the web browser will display this. This is the credential for that ISRM-WAF-Role, it's just showing up right in the browser.

And if you copy and paste the pieces of this and put them into the Amazon -- Amazon Web Services client software, then that client software will allow you to go and execute the different functions that this credential is allowed to do, like accessing the S3 bucket in this example.

Q. So she could have acquired the same credentials through her web browser?
A. That's right; using just these three steps, setting up the proxy server and then simply navigating to that IMS IP address.
Q. And how long did that one, two, three take you?
A. Takes two or three minutes. I could demonstrate it right now if people had attention for it, but -- but the key thing is that all of this still works in Amazon today. It still works with the Apache server today. These aren't bugs in the services that have been corrected and patched as a result of knowing what Ms. Thompson could do; it's just a matter of how each of these computer systems is configured and whether they're configured to allow these different steps to take place.
Q. And you don't have to use a TOR or VPN to do this?
A. No, no.
Q. And she didn't have to use those services to do what she did?
A. No. And in fact, using TOR or VPN probably would have made her accesses even more visible, even more likely to set off alarm bells at the different entities. A lot of people are looking for access from TOR or from certain VPNs.
Q. And you saw on some of the exhibits the government went through with the witness, there was a response --
MR. KLEIN: We can pull this down for a second. Thank you.

Q. (By Mr. Klein) There was response to a command from one of her scripts was like unauthorized or forbidden. What was happening there?

A. Well, when a server is returning and saying it's unauthorized, the connection, the command, is unsuccessful in general. I'm sure everyone has had this happen to them sometime or other while following a link on the web, you get an error message like that. It just means the server said no to the request.

And reviewing, there was a script that Ms. Thompson ran that appeared to be -- she was investigating what capabilities were allowed by the credentials, by the roles that she -- that the servers had allowed her to access. And each command that she sent either succeeded because the role had been configured by the customer to allow that action, or it did not succeed, the command didn't go through, because the role said no.

Q. And just so I understand, like when you arrive there, you don't get like a list of what works and doesn't work, this is the -- how you would figure that out even, for anybody who arrived there?

A. That's right. In general, the computer -- the way Amazon works, you, as a user with a role, are not presented with the policy that says what that role can do. You can attempt commands and the server can be configured to allow you to proceed or not.

Q. And you didn't see any evidence she like went past -- when there was an unauthorized or forbidden, you didn't see evidence she tried to go past that point?

A. To somehow override those places where it said -- no, I didn't see any evidence of that.

Q. Okay. Do you recall Mr. Ho talked about an SSRF attack, server-side request forgery attack?

A. Yes.

Q. And do you recall that there was testimony about he thought what happened here was one, and on cross he, Mr. Schmidt of AWS, did not. Was what happened here a server-side request attack; is that accurate?

A. I don't think that that's technically accurate to classify it as SSRF.

SSRF by analogy to cross-site scripting, which we abbreviate as XSS, is a kind of vulnerability that happens at the web application layer.

What's happened here is at a different layer of the network stack. It's not a bug in a web application where it's failing to validate a URL that a user has provided; instead, it's simply that a server has been configured to act as an open proxy.

And then we technically have a different classification for an open proxy that maybe someone didn't intend, but you can't tell just by looking at it whether it was intended or not, than we do for a server-side request forgery vulnerability.

Sometimes people, again, like SOCKS proxy and HTTP proxy, people speaking loosely conflate those terms. And I don't fault Agent Ho for perhaps being imprecise.

Q. Let me show you -- it's our last exhibit.

MR. KLEIN: And this is for demonstrative purposes again, Your Honor, 1206.

THE COURT: 1206, let me see it, first, is admitted for demonstrative purposes and can be displayed.

Q. (By Mr. Klein) So if you could walk the jury through this exhibit, that would be appreciated

A. Yes. So this is a summary of the three different kinds of computer systems that Ms. Thompson interacted with and the way they were configured and the types of requests that she sent to them. And this is going to show that the request that -- whether the request that she would have sent to these different computer systems complied with the rules that were configured in each of those systems.

So to review, Ms. Thompson started by talking to these open forward proxies running on EC2 instances, such as Capital One's WAF.

Q. And this applies for all the alleged victims, this summary?

A. Generally, to all of the alleged victims. They were all running in some form an open forward proxy.

In Capital One's case, this was the Apache software. It was configured to allow anyone to use it to make requests to

other servers, including to the IMS computer system.

Okay. Then we have the Instance Metadata Service, IMS, computer system that Amazon runs internally. And for all of the alleged victims, they had configured IMS to provide role credentials in response to requests from the alleged victims' EC2 instances.

Finally, we have the other AWS services like S3 and EC2 that in each of the alleged victims, they had configured their role credentials so that anyone possessing those credentials was allowed to either read data, or launch EC2 instances, or perform various other kinds of actions for which those roles had been explicitly granted permission. The roles, by default, would have no permission.

Q. And it says "Paige" there, but that could have been another member of the public?

A. That's right.

But in each of these cases, I note that these rules that are listed here are not the default rules. The defaults in each of these cases would be not to provide these acc- -- this kind of access. In each case, the alleged victim needed to make some changes to specifically configure these systems to provide this kind of access.

Q. So in each case, they gave permission for Ms. Thompson to download data?

A. In each case, they set a rule. And the effects of those

rules I've listed to the right in this diagram.

When Paige Thompson made a request to the open forward proxy, she asked that proxy for -- to make a request onward to the IMS system and ask for available credentials. That's what happened and it's what the open forward proxy was configured to allow Ms. Thompson or any member of the public to do. So her request complied with that configured local rule.

Next, the Instance Metadata Service received that request from the open forward proxy. The request to provide -- to send the available credentials, since it was configured to provide credentials in response to requests from the EC2 instance, it complied. That request complied with the rule. The server said, okay, and it returned the credentials, which the proxy server then returned to Ms. Thompson's computer.

And then in the bottom row there with the other AWS services, Ms. Thompson could, in general, just speak to them directly and say, here's a credential that I'm in possession of, please send me data or launch an instance or perform other functions. And in the cases where that role and that credential had been authorized to perform those actions, again, the request complied with that computer system's rule, that computer's rule. And so it said, okay, and allowed that request to go through.

Q. So in each case, each of these systems complied with the rules --

A. That's right.

Q. -- their internal rules?
A. There's not a bug. There's not a bug in any piece of this software that Ms. Thompson is exploiting. She's not sending an -- some kind of exotic invalid command that is unanticipated by the programmers of these individual computer systems that is exploiting them. Each of these commands is compliant with the configured rules and is being processed normally by this different system.

MR. KLEIN: Nothing further, Your Honor.

THE COURT: Okay. Assistant United States Attorney Manca, cross-examination of Professor Halderman.

CROSS-EXAMINATION

BY MS. MANCA:

Q. Good morning, Dr. Halderman, still in morning.

I'm going to get some water myself.

A. And good morning to you as well.

Q. Thanks.

So your first job out of school was at the University of Michigan?

A. I suppose I had summer jobs before that, but my first full-time job was as a professor; that's right.

Q. And so your entire career has been in academia; correct?

A. Well, while I've been a professor, I also founded two companies, one that provides security services to about 300 million websites, and the other of which uses Internet-wide

scanning to provide security information to companies and try to keep them safe.

Q. That last company is called Censys?

A. That's right.

Q. And you cofounded that company?

A. I did.

Q. And you have a financial stake in that company?

A. I do. I still -- I own some equity in the company. I don't work there day-to-day.

Q. Okay. And your company actually just completed a $35 million round of series B funding?

A. I understand that from the press, but I don't have day-to-day involvement.

Q. Okay. And Censys commercialized ZMap; is that correct?

A. Censys doesn't actually use ZMap, but it uses other more advanced scanning tools that are based on the work that we did in our research about ZMap; that's right.

Q. Okay. Your resumé specifically says that Censys commercialized ZMap, quote?

A. Well, it commercialized the techniques behind it.

Q. Okay. But your resumé says Censys commercialized ZMap; is that accurate?

A. I don't have my re- -- I'm not -- if it says that, it says that.

Q. Okay.

A. I don't think it's unfair to say that it commercialized it, but just trying to be technically accurate.
Q. Okay. So fair to say, then, that you have a financial stake in the success of Internet scanning technology?
A. I mean, I suppose so. Censys -- what Censys does is about taking data from Internet scanning, but then using that to provide -- to provide what's called web attack surface management. We let companies know about what they are exposing to the world through clouds like AWS.
Q. Okay. But ZMap, when it scans the Internet, doesn't download data; correct?
A. You can configure the ZMap tools to download data, and a lot of people use it in that way.
Q. Okay. But a person would not configure ZMap to download someone's data without permission, would they?
A. They could, and there are research studies in which that is done. You can tell by looking at a piece of data just as an Internet client. You can't tell in general whether you're allowed to download it or not. It's either the server returns it to you or it doesn't.
Q. Okay. And you agree that scan practitioners should not exploit vulnerabilities or access protected resources; right?
A. Well, I think that's a general rule of thumb that we use in research about that, that -- you know, I myself have written about guidelines for being a good neighbor or being a good

citizen online and for other research practitioners, and what we -- our rule of thumb in the field is -- our rule of thumb in the field is we're not attempting to exploit vulnerabilities.

Q. So you mentioned the practices for good Internet citizenship. These include coordinating closely with local network admins to reduce risks and handle inquiries; right?

A. That's right.

Q. Signal the benign nature of the scans, yes?

A. Yes. So that the idea there is to make it easy to find out that this is a -- for instance, what you're referring to, again, I believe this is coming from the original research paper where we introduced the ZMap tool, where my students and I made recommendations to other people who are running this about, you know, how can you be -- how can you be a good neighbor online when you're using a tool like this. And we're making these recommendations to other researchers.

They're certainly not hard-and-fast rules. I know -- you know, even we, I admit, have not always followed all of these rules in our own research because they're not, you know, universally applicable. And they're certainly not things that everyone who uses our tools follows all the time, but I think they're good practices. They're good prosocial recommendations.

Q. Okay. So when ZMap scans, it signals the benign intent of the scan by identifying itself on Whois entries and DNS records; right?

A. No, that's not how ZMap works, but that's our recommendation for a user of the ZMap software, especially in an academic environment where you have the resources to do things like set up your own Whois records and reverse DNS, but a hobbyist, an amateur using the tool at home, probably wouldn't be able to easily do that if they're using it from their home Internet connection.

Q. And you recommend conducting scans no larger or more frequent than is necessary for research objectives; correct?

A. That's right.

Q. Okay. And both good-faith researchers and malicious hackers use proxy scanners to find vulnerabilities; right?

A. I suppose so.

Q. And the most alarming malicious potential for high-speed scanning lies in its ability to find and exploit vulnerabilities en masse in a short period of time?

A. Yes. And there are certainly people who also use Internet scanning for malicious purposes.

Q. And in fact, you're aware of situations in which malicious attackers have used ZMap and similar scanning technology to find and exploit vulnerabilities?

A. That's true.

Q. And you wrote that maintaining the utility of scanners for defensive security research, while simultaneously protecting networks from attack, is a difficult challenge?

A. Yes, I did.
Q. You mentioned that you've written a lot of reports over your career; is that right?
A. Yes.
Q. One of the reports you wrote was about vulnerabilities in Dominion voting machines?
A. I have written a report about that in the context of other litigation; that's true.
Q. Okay. And so in 2016, that report was used by Jill Stein of the Green Party to challenge election results in Michigan and Pennsylvania; true?
A. No, that's false.
Q. Were you an expert in litigation on behalf of Jill Stein, challenging election processes in Pennsylvania?
A. Yes, I was.
Q. Okay. And in fact, a federal judge dismissed that lawsuit in April of 2020?
A. In April of 2020? That may be correct, I'm not sure. I've been involved in -- I've been involved in a number of different litigation matters.
Q. And you testified in that lawsuit, Jill Stein's lawsuit?
A. In the Stein Pennsylvania lawsuit, yes.
Q. Okay. And in the federal judge's order dismissing that lawsuit, he described your theories as --
MR. KLEIN: Objection, Your Honor, another judge's

order is irrelevant.

THE COURT: Overruled.

You can ask the question.

Q. (By Ms. Manca) In the federal judge's order dismissing the lawsuit, he described your theories as, quote, ill-considered and daft?

A. Excuse me, I don't mean to -- it's funny phrasing. I don't mean to laugh at it.

Q. But that's correct that that was the phrasing that was used in this opinion?

A. So that's a very different kind of case. That was a highly politically charged case, unfortunately, where my role was about certain technical matters and -- where my role was about certain technical matters, and that was the -- that was what the judge wrote.

Q. He found your testimony was not credible?

A. I don't have the ruling in front of me.

Q. Do you remember that he found your testimony not credible?

A. I don't -- I don't remember exactly what he wrote.

Q. Do you remember that he wrote that you acted more like an advocate than an expert?

A. I don't remember what he wrote.

Q. Okay. Would looking at a copy of the opinion refresh your memory about that?

A. It might.

MS. MANCA: Your Honor, may I approach?

THE COURT: Yeah, sure.

THE CLERK: What number would you like, Counsel?

MS. MANCA: 970, please.

THE CLERK: 970.

Do you have a copy for Judge Lasnik?

THE COURT: Do you have a copy for me?

MS. MANCA: Oh, yes, I do.

THE COURT: Thank you.

MS. MANCA: I apologize, Your Honor.

THE COURT: That's all right.

Thanks, Victoria.

THE WITNESS: Thank you.

MS. MANCA: Thank you.

Q. (By Ms. Manca) Dr. Halderman, could you refer to page 22 of that opinion?

A. Yes.

Q. So, Dr. Halderman, does that refresh your memory about what the judge wrote in the opinion?

A. Yes.

Q. And it's true that he wrote that you acted more like an advocate than an expert; correct?

A. That's what the judge wrote.

Q. And the judge said you routinely offered opinions without factual basis to bolster Stein's litigation position and

repeatedly tried to avoid answering questions when the truthful response might not help Stein; is that also correct?

A. That's what he's written here.

And I will say that I've served as an expert in many different litigation matters and my testimony has also been cited very favorably in other rulings.

Q. I'd like to ask you about the University of Michigan policy on responsible use of its information resources.

A. Please.

Q. Yeah.

The University of Michigan policy says that members of the university community should use only those computing resources that they have been authorized to use, and use them only in the manner and extent authorized; is that correct?

A. That's the policy of the University of Michigan.

Q. It says, Do not interfere with the intended use or proper functioning of information technology resources?

A. Yes.

Q. It says, Do not gain or seek to gain unauthorized access to any resources?

A. Yes, that's what the university's policy is.

Q. It says, Do not circumvent or bypass security measurements, requirements, or any standard protocols in place to ensure the confidentiality, integrity, and availability of University of Michigan systems and networks?

A. The university has a lot of policies that go beyond what the law requires.
Q. Okay. And Ms. Thompson's conduct in this case would have violated University of Michigan policy, would it not?
A. Perhaps, if that's what the -- if her conduct had -- I'm not sure. But her conduct, apparently, was not directed at University of Michigan.
Q. I want to ask you about the technical aspects of the attack.
You referred to this as a forward proxy in your direct examination; correct?
A. As an open forward proxy; that's correct.
Q. Okay. You also testified about Steve Schmidt's characterization of this attack?
A. I did, yes.
Q. Okay. And Steve Schmidt is the chief information security officer for Amazon Web Services?
A. That's right.
Q. Okay. And Amazon Web Services, or Mr. Schmidt on behalf of Amazon Web Services, called this "an open reverse proxy attack"; correct?
A. Again, he's speaking imprecisely, and that's not technically correct that it was an open reverse proxy.
Q. Okay. So you disagree with the chief information security officer of Amazon?

A. I do because it's just -- that's not what a reverse proxy is. A reverse proxy, the server is in control of what other computer, the proxy server, is retrieving the information from.

Q. Okay. I want to ask you a hypothetical really quickly: Let's say someone steals my bank account and my PIN number, okay, that person enters the stolen numbers into the online bank account, accesses my bank account, downloads all my money, each step of that system worked as intended; right?

MR. KLEIN: Objection for relevance to this case, Your Honor.

THE COURT: Overruled.

You can answer, but you don't have to just say yes or no.

A. All right. I mean, that's your hypothetical. I'm not sure that I really want to offer an opinion about -- about a speculative case like that because that's -- that's not what happened here.

Q. (By Ms. Manca) Okay. But if someone uses a stolen password to enter it into a system, be it Gmail, be it a bank account, and the system processes that stolen password, the system is working as it's supposed to; right?

A. But the -- the pass -- in that case, there is a stolen password, and there is not a stolen password at issue in any of these systems.

Q. Okay. But if -- if the password were stolen, that would be problematic; correct?

A. Again, that's, you know, not what happened here.
Q. And then if the person then has unauthorized access to my bank account and enters a command to download my money, the system would also be responding to that command; correct?
A. I don't believe Ms. Paige [sic] is accused of accessing anyone's bank account.
Q. She's not, but I was ask- --
A. Ms. Thompson, excuse me.
Q. Uh-huh. She's not. But I'm asking if a thief inside a bank account entering a number -- entering a command to withdraw money, and the system responds to that command, everything is working as the system is designed; correct?
A. Presumably the crime is the theft of the money, but I'm not a lawyer.
Q. Okay. And the crime is the unintended consequence of someone having money that they're not entitled to?
THE COURT: Ask another question, Ms. Manca.
Q. (By Ms. Manca) I wanted to talk to you about Amazon's Instance Metadata Service. That cannot be accessed directly by an external user; is that right?
A. Its only addressable from the local EC2 instance.
Q. And so none of the companies that testified in this case, and you were here for their testimony, none of those companies knew that the Instance Metadata Service could be accessed in this particular way; that is, through a proxy?

A. None of them knew? I'm not aware of their state of knowledge.
Q. None of these companies wanted an external user to access the Instance Metadata Service; correct?
A. Well, people configure their computers all the time in ways that allow other people to do things they might not have expected.
Q. So it was unexpected that the proxy hit the Instance Metadata Service; correct?
A. It's quite possible that it was a mistaken configuration on some of their ports. People mistakenly publish things they wish they hadn't all the time.
Q. Okay. And this vulnerability was an unintended consequence of the way they configured their proxies?
A. People make mistakes on the Internet all the time.
Q. Uh-huh.
None of the companies knew that this particular vulnerability existed?
A. I'm not aware of their state of knowledge, but that's completely possible that they weren't aware. But it doesn't seem to me that -- it doesn't seem to me that -- the law possibly could be that it's a crime to do anything on the Internet that someone else didn't intend to be possible.
Q. Well, so let's talk about that, because for several years you've worked with legal teams to petition the United States

Copyright Office to create and expand security research exemptions to the Digital Millennium Copyright Act; correct?

A. I have, that's right.

Q. And your most recent advocacy was in 2021?

A. I think that's right.

Q. Okay. And in your comment to the digital -- or, I'm sorry, the Office of the Registrar, you use the term "good-faith security research" over 60 times. Does that --

A. I think that's right, yes.

Q. -- more or less --

A. Yes.

Q. Okay. So you never wrote "security researcher" by itself, did you?

A. I don't know. That's possible.

Q. You would always say "good-faith security researcher"; right?

A. Well, this is in the context of a very specific legal question. And basically, what these exemptions are about is there's another federal law, the Digital Millennium Copyright Act, that confers criminal liability or civil liability onto many different kinds of acts that are indisputably prosocial -- prosocial defensive security research. They're things that keep people safe.

And there's an elaborate mechanism that congress included in the law whereby it's possible for advocates or members of the

public or affected parties to petition the registrar of copyright, the Registrar of Copyrights for an exemption to this set of restrictions. And so I've worked with a legal clinic at the University of Colorado several times to try to get the copyright office to grant this kind of exemption for different kinds of good-faith security research is what we call it. And I've testified to the -- the copyright office about that on several occasions. And they've granted different forms of exemptions several times.

Q. The "good-faith" part is important, isn't it?

A. Yes. There's certainly things that can be done in bad faith that are not prosocial security research.

Q. Okay. And that's the limiting principle -- that's the balance between the interests of security researchers and the vulnerable companies; right?

A. That's right; it's difficult sometimes to draw the line, but there is a general notion that work is being done in order to ultimately make people more secure or get problems fixed.

Q. And good-faith security researchers follow strict norms and customs; right?

A. There are customs, especially as people become more educated and professional in this field. They're not all things that people know when they're starting out.

Q. You wrote in your comments to the DMCA, "good-faith security researchers follow strict norms and customs"; correct?

A. Again, the norms and customs are things that people, as they become more involved in a community, are going to understand better, but, yes.
Q. Okay. So your answer is "yes," good-faith security researchers follow strict norms and customs?
A. That's what I wrote.
Q. In the course of research, if a researcher finds insecure or troubling information, that researcher follows norms of responsible disclosure?
A. In general, yes.
Q. Okay.
A. But they're norms. Again, they're not hard and fast that apply to every situation.
Q. Okay. But you previously described them as strict norms and customs?
A. I don't think that's incompatible with them being norms and customs. It doesn't mean they apply to every situation. A norm or a custom is something that has a general form and doesn't necessarily apply to every specific case.
Q. Responsible disclosure includes informing the host entity of the discovered vulnerability?
A. In general, yes, but not always.
Q. And researchers follow ethical norms in the field, which include obtaining consent from operators of systems where needed to avoid harm to the users of the systems; correct?

A. Pardon me?
Q. Researchers also follow ethical norms in the field, which include obtaining consent from operators of systems where needed to avoid harm to users of those systems?
A. That's generally true, yes.
Q. And norms and customs of academic research require that you only attempt to exploit vulnerabilities with the prior permission of the owner of the system?
A. In general, that's right. We have -- we have stricter norms in academia than apply in general. And certainly, our norms go beyond what the minimal -- minimum that the law requires of us. We're -- for instance, we're required to comply with institutional review board requirements that have to do with the protection of human subject data; we may have local university rules like you cited for the University of Michigan that also go beyond the minimum that the law would require, and we have professional norms that within our scientific community we've developed. And that's what that is all referring to.
Q. When did you become involved in this case?
A. I don't remember, probably approximately in 2020.
Q. Getting back to the users of these systems, Capital One didn't want its data downloaded; correct?
A. The data at issue, you mean?
Q. Yes, the data at issue.
A. Yes, I take it they didn't.

Q. Apperian and Digital.ai, they didn't want the data at issue downloaded; correct?

A. I take it they didn't, either; that's right.

People accidentally or not wanting to -- not wanting to publish things, unfortunately, do mistakenly make data and other things public on a regular basis. I found such data in my own work.

Q. 42Lines didn't want its data downloaded?

A. I take it they didn't.

Q. Bitglass didn't want their data downloaded?

A. I take it not.

Q. And Survox didn't want its data downloaded?

A. No.

Q. Capital One didn't want its role credential used by Paige Thompson; correct?

A. You mean after the fact or before the fact?

Q. Before the fact.

A. I'm not sure that Capital One had thought through what the implications of its configuration choices were.

Q. Apperian didn't want its role credential used by Paige Thompson; correct?

A. Again, I'm not sure that any of the alleged victims had thought through what the consequences of the different choices and configurations they made were before Ms. Thompson's conduct brought those implications to their attention.

Q. So the fact that these companies didn't want their data downloaded and that they didn't think through the unintended consequences of these configurations, that doesn't affect your analysis at all?
A. That doesn't affect my analysis of whether the systems were behaving the way that they had been set up to behave.
Q. What about the fact that Paige Thompson knew she was not supposed to have access to these credentials, does that affect your analysis?
A. So, again, I think, you know, what was in Ms. Thompson's mind is -- I can only speculate about.
Q. Do you think it's acceptable for someone to exploit a vulnerability, even if they know it's wrong?
A. I don't think I'm offering an opinion about the morality.
Q. Do you think it's okay for someone to access private internal information, even if they know they shouldn't be accessing that information?
A. I think it depends on what they do with it as a consequence of that. If they've made -- I know -- I myself and other researchers in academia sometimes do run into information that isn't intended to be public, that it's pretty clear to us afterwards isn't intended to be public.
In cases where that information is important, we try to take steps to let the people know about it so they can fix it.
Q. Is your view that if a company makes a mistake, then

anything that happens after that point is their fault?

A. In some consequentialist sense, I suppose that's true that it is their fault, but the question here seems to be what does the law require.

(Off the record.)

MS. MANCA: I don't have any further questions. Thank you.

THE COURT: Thank you, Ms. Manca.

Any follow-up, Mr. Klein?

MR. KLEIN: Yes, Your Honor.

THE COURT: We'll go a little over noon just to finish this off.

REDIRECT EXAMINATION

BY MR. KLEIN:

Q. Good morning again, Professor Halderman. Let's talk about the Michigan case again. Was that a highly charged political case?

A. Yes, unfortunately.

Q. And did you refuse to answer any of the judge's questions or the prosecutor's questions today?

A. I don't believe so.

Q. Okay.

A. I've certainly tried my best. If there are any further questions, I'm happy to do my best again.

Q. And were you also involved in another case later in Georgia

where the judge found your testimony credible in about the same kind of politically charged issue?

A. Yes.

Q. And that's because this relates to the last election?

A. The last several elections.

Some of my work is about the security of election systems specifically where, unfortunately, there's a lot of false information out there, and the politics can become quite charged.

Q. And your testimony about that has nothing to do with network scanning, like the things we're talking about here today?

A. No. It's a very different kind of issue.

Q. Okay. And -- oh, sorry.

The prosecutor asked you about what these companies may have intended, but, again, let's return to how their systems were set up and configured. Did they permit Ms. Thompson or any member of the public to do the steps we talked about?

A. Yes. Each of their systems was configured to allow the actions that Ms. Thompson took to succeed.

Q. And as part of your research, do you often have companies come after researchers for finding flaws or vulnerabilities?

A. Yes. That has happened many times to people who are security researchers in my broader community.

Q. Do they often go tell their story to law enforcement and

try to get law enforcement to come after good-faith security researchers?

A. And that happens, unfortunately.

MR. KLEIN: Your Honor, I have -- I think the government opened the door to something that I wanted to discuss with Your Honor, but, I don't know, was the basis of a prior ruling.

THE COURT: Is that the last item?

MR. KLEIN: Oh, no, it's not, Your Honor.

THE COURT: Do the other one.

Q. (By Mr. Klein) The prosecutor talked to you about how there seems to be some disagreement about whether this was a reverse proxy or forward proxy. How do you know, from a technical perspective, this was an open forward proxy?

A. Well, because the command -- the curl command would not succeed if it was a reverse proxy, it just couldn't possibly. There's no way that the -- without that forward proxy capability being enabled that a party sitting outside of AWS, such as Ms. Thompson, could address the IMS system.

Q. And is that because you've reviewed the commands and reviewed the evidence in this case?

A. That's right. And you can look right in the documentation for the Apache web server, it clearly describes the difference and the way that the -- a forward proxy versus a reverse proxy behaves. This is indisputably a forward proxy.

Q. Does this case have anything to do with an ATM machine?
A. No.
Q. Does it have anything to do with a PIN for an ATM?
A. No, I don't think so.
Q. Was a PIN required for anything that Ms. Thompson did?
A. No.
Q. Was a password required for anything Ms. Thompson did?
A. Not for any of the steps that I've described.
Q. So that analogy was completely off point for what we're talking about here today in terms of the technology and the configurations?

THE COURT: That question is objectionable, Counsel.

MR. KLEIN: Your Honor, just the point I was going to raise, but I'm done now.

THE COURT: Okay. So, Victoria, how about we just take the jury out there so they can see the nice hallway and look across at the apartments and stuff, and I'll deal with this, and then bring them back, okay?

THE CLERK: Okay.

THE COURT: Leave your notepads right on your chairs.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Okay. Please be seated.

And, yes, thanks, Mr. Klein, for bringing it up outside the -- with a little notice to me.

So what's the area?

MR. KLEIN: Your Honor, I wanted to talk to Professor Halderman for a moment about the fact that Ms. Thompson did signal through her scanning to Capital One. And I wanted to ask questions about that, and I also -- through the note and through the messaging with Ms. Valentine, because I think there is evidence. And the clear implication of the prosecutor's questions I thought was that, you know, good-faith researchers do signal and that, therefore, they're going to argue in close Ms. Thompson didn't signal at all. And I think Professor Halderman would say, if I ask him, that there are certain steps Ms. Thompson took here that should have signaled to Capital One what was happening here.

THE COURT: But he's already testified to that regarding the note, that he said Capital One, when they saw that note --

MR. KLEIN: There is a scan she did, Your Honor, after the note was passed that I think would Mr. -- again, I can't speak for him, but I think he would testify that it was a loud and proud scan or what they call a confession scan. It's a type of scan you do when you want the other side to know that you're looking at their -- and I'm -- be his words, not mine, but sort of you're out there and you're signaling to them, because she did ask about signaling to people. When you scan, you signal.

THE COURT: Well, I mean, it's two separate issues.

One is did Ms. Manca open the door. No. You brought that issue up on direct and she cross-examined. So there was nothing about opening a door.

The second issue is, would it have been relevant for you to bring it up in direct examination, and I think it would be.

So I'll let you do it because -- but not because Ms. Manca opened a door; you understand?

MR. KLEIN: Happy to do it for any reason.

THE COURT: Okay. But not -- let's go back to the note, because you've already covered that.

MR. KLEIN: I won't go back to the note.

THE COURT: Just the so-called confession scan.

MR. KLEIN: I'm just going to ask him if there's any evidence that he's reviewed that indicate that Ms. Thompson signaled scanning.

THE COURT: Okay. All right. That's fine.

And then you're done?

MR. KLEIN: Then I'm done, Your Honor, yes.

THE COURT: Yes.

And are you going to have more cross?

MS. MANCA: I might briefly.

THE COURT: Sure.

And then does the government know yet whether it's going to do any rebuttal witnesses?

MS. MANCA: We do, Your Honor. We will likely rebut

with John Strand and Waymon Ho.

THE COURT: And are they all ready to go --

MS. MANCA: They are.

THE COURT: -- or do you want to do that after lunch?

MS. MANCA: After lunch would be preferable, Your Honor.

THE COURT: Okay.

MR. KLEIN: And we want an offer of proof about what they're rebutting, Your Honor, if it is truly rebuttal.

THE COURT: I'm not going to send the jury home, that's the only reason I'm asking about that, so we'll bring them back.

Okay. You can bring them in, Victoria.

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Okay. Mr. Klein, you can go ask a few of those questions that we talked about.

MR. KLEIN: Yes, Your Honor.

REDIRECT EXAMINATION

BY MR. KLEIN:

Q. In conducting your review of the evidence, did you see evidence of signaling?

A. Of signaling?

Q. Through scanning?

A. Yes.

Q. Can you talk about that?
A. Yes. So in -- in the -- in the logs that Capital One provided, you can look at the timeline of those logs. And Ms. Thompson discovered the configuration issue in March, subsequently downloaded the data, and that it appears that she came back again in April and conducted a relatively aggressive series of commands. And by "aggressive," I simply mean she executed a larger number of commands that would have created more log entries on Capital One's side that might have set off -- that might have set off monitoring systems on their side that would be likely to -- more likely to alert Capital One to the fact that their systems had been configured in this way.
Q. And did you see evidence that Capital One described these as confession scans or loud and proud scans?
A. Loud and proud scans, I remember seeing that in some of the discovery documents; that's right.
Q. And what does loud and proud scan mean, just to be clear?
A. Well, a loud and proud scan would be a scan that's -- that's tuned to try to set off detection systems, like to notify, to alert the party being scanned that they may have a configuration they don't intend.
Q. And that's consistent with the signaling scanning we were sort of -- Ms. Manca was talking with you about?
A. Well, that's right. What she was referring to in terms of signaling your identity in -- as a -- as a scanner, it's

something like we do at the university, we have messages that someone who receives or a scan can see this is part of a university research study.

The reason we do that is because companies review their own logs and sometimes notice that they're being scanned and wonder, do we have a security problem, should we spend resources to try to investigate whether we are under attack or whether we have a configuration problem or a vulnerability. And we want to signal to them that -- the benign intention of our research activities so that they don't waste their resources trying to investigate.

But in the scan that Capital One calls a loud and proud scan, I think it's likely trying to do the opposite, trying to set off those logging monitoring detection systems so that Capital One has an opportunity, is alerted to the fact that there is this configuration problem.

MR. KLEIN: Nothing further, Your Honor.

THE COURT: Ms. Manca, any further questions?

MS. MANCA: Very briefly.

RECROSS-EXAMINATION

BY MS. MANCA:

Q. Ms. Thompson could have configured her scanner to identify herself; correct?

A. She could have. I'm not sure that that would have made the problem any more likely to be detected in this issue.

As I say, the reason that we identify ourselves as

researchers in our research scans is so that people don't waste time investigating. And if anything, Capital One should have spent more time investigating.

Q. And it's possible that this scan was to determine if the vulnerability still exists; correct?

A. I think it's likely that some of the activity was to try to determine whether the vulnerability had been fixed yet so that Ms. Thompson could decide whether to take further steps to try to alert Capital One about it.

Q. Okay. But you're making an assumption regarding her intent in making that statement?

A. That's my analysis based on the pattern of scans and the apparent attempts to notify Capital One that occurred.

MS. MANCA: No further questions.

THE COURT: Okay. Done?

MR. KLEIN: Nothing further.

THE COURT: Yes.

We'll take the lunch break now. The government -- is the defense ready to rest its case?

MR. HAMOUDI: Yes, Your Honor, we're ready to rest.

THE COURT: So the defense has rested its case.

The government has an opportunity to present what's called rebuttal evidence. We're not sure they're going to do it or not, but I want them to have time over the lunch hour to think about it.

So please be back at 1:30.

And, Victoria, should we just make them go in the hallway again?

Just kidding. You go back to Judge Pechman's courtroom at 1:30 and Victoria will bring you over.

Either we'll hear relatively brief testimony and I'll send you home, or I'll send you home.

And by tomorrow -- we're going to work on jury instructions for the rest of today and other legal matters, and then at 9:00 tomorrow we'll instruct the jury, do closing arguments, and submit the case to you.

Now, you know, there's 15 of you and juries of 12 decide things, so three alternates will not be starting the deliberations. But if something were to happen to one of the 12 deliberating jurors, those people could still be substituted in and the deliberations begin anew. So I still need you all to be part of the system, even if you're not back in the jury room for deliberations.

So thank you for your patience again with us this morning. Please be back in Judge Pech- -- Zilly's courtroom, not Judge Pechman, at 1:30.

Thank you. You're excused.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: So, Mr. Friedman, Ms. Manca, Ms.

Culbertson, you don't have to say what you're going to do right now, you want to talk to the people. But when you know if you're going to do it, let defense know and let Victoria know.

And if you are going to present rebuttal testimony at 1:30, we'll have you put on the record what that testimony will be outside the presence of the jury. And if there's an objection, I'll rule on that, okay?

MR. HAMOUDI: Your Honor, just for the record, I believe I need to renew my motion for judgment of acquittal on all counts in the second superseding indictment under Rule 29.

THE COURT: Okay. Thank you.

We're all done. Thank you.

See you at 1:30. That's fine; 1:30 is fine.

(Court in recess 12:16 p.m. to 1:33 p.m.)

THE COURT: Okay. Government rebuttal testimony?

MS. MANCA: Yes, Your Honor. We would like to call Waymon Ho and John Strand in rebuttal.

THE COURT: In what areas are you offering the testimony to rebut?

MS. MANCA: Yes, Your Honor.

As to Waymon Ho, we are offering his testimony regarding Defense Demonstratives 1204 and 1205.

THE COURT: Okay.

MS. MANCA: And then regarding John Stand's, there was testimony regarding systems functioning as intended and whether

a programming error is distinguishable from a misconfiguration, and we would offer John Strand's testimony on those two points.

THE COURT: Okay. Mr. Klein?

MR. KLEIN: Your Honor, we object under Federal Rule of Evidence 403. They had the chance to put this all out in their opening. They did discuss it, actually, in their case-in-chief.

They didn't challenge -- with regard to the exhibits, Ms. Manca didn't raise any challenges of those exhibits during her cross-examination. She cross-examined about nothing technical.

And with regard to Strand, again, this all came out in their case-in-chief. This is all cumulative, it's not new. They put this evidence already in, and we would oppose it under 403.

THE COURT: Okay. I'll definitely allow Agent Ho to talk about those exhibits that were utilized by Professor Halderman.

In regard to Mr. Strand, I'm not exactly sure what you mean, Ms. Manca. Could you be more specific?

MS. MANCA: Yes, Your Honor. There were questions in direct examination of Dr. Halderman that this was not a bug, creating, in our belief, a false distinction between a bug and a misconfiguration as allowing access.

There was also testimony about everything functioning as

intended, and a mistake is not something that functions as intended, and the testimony would rebut that principle.

THE COURT: Okay. I'm going to definitely allow Agent Ho. I'm not convinced that Mr. Strand's testimony is actually rebuttal. I think it is cumulative. So just Waymon Ho. Okay?

MS. MANCA: Okay.

THE COURT: All right. And then that will complete the rebuttal testimony.

The defense has rested.

We will dismiss the jury and deal with legal issues and our jury instructions from that point, on.

All right, Victoria, you may bring the jury over.

Mr. Friedman, we're not going to deal with forfeiture until after the verdict, correct?

MR. FRIEDMAN: Yes, Your Honor, that's correct.

THE COURT: And then part of it is the Court's and part of it is the jury?

MR. FRIEDMAN: Yes.

THE COURT: And the defense may be not contesting, but that's for later, right?

MR. HAMOUDI: Yes, Your Honor.

THE COURT: Okay. Got it.

And have we agreed on the admissibility of that AWS model contract?

MR. HAMOUDI: Yeah. We have the contract, and since we closed, Ms. Manca said we can reopen and just move the contract in as the next exhibit.

THE COURT: It's just moving the exhibit into evidence?

MR. HAMOUDI: Yes.

MS. MANCA: And with the stipulation that this is the governing contract for the victims in the case.

THE COURT: Okay. Great.

And according to my records, the alternates are -- Alternative No. 1 is Seat 15, Alternate 2 is Seat 9, and Alternate 3 is Seat 12. I know the government was unhappy that I let them pick, but I think they're all new people in those chairs. So those will be the alternates. I feel bad, because some of them have been the most alert jurors, but that's what we did.

MS. MANCA: You know, can I raise one more point with respect to John Strand's testimony?

There was no expert disclosure in the case, as the Court is aware, and so that's another reason that we believe that this is properly the subject of rebuttal testimony, is that Mr. Halderman's testimony was not anticipated due to the lack of disclosure.

THE COURT: Okay. I'll think about it, Ms. Manca.

MR. FRIEDMAN: Your Honor, could I supplement that?

THE COURT: Sure.

MR. FRIEDMAN: It's sort of a central point, in we had asked for -- obviously, the decision not to have expert disclosure was the defense's, but so things are coming up for the first time on the stand that we had no knowledge of.

If the Court looks at the disclosure provided in the trial brief, there's nothing there. It is a central point on a central issue, and we think Mr. Strand would be about 15 minutes.

THE COURT: Okay.

MR. KLEIN: Your Honor?

THE COURT: I'm not changing my ruling.

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Thank you. Please be seated.

The Court is allowing the defense to reopen to move to admit a stipulated exhibit.

Mr. Hamoudi? What is the next number?

THE CLERK: 1207.

THE COURT: We'll figure out the numbers, but this is a sample AWS contract that they enter into with all of their clients. It's a blank contract because it's not particular to any company, but it is the one that Amazon Web Services used with all of their customers.

THE CLERK: Your Honor, this is 1207.

THE COURT: 1207 is the sample contract, and it is

admitted into evidence by agreement of the parties. Okay?

1207.

(Defense Exhibit 1207 admitted.)

THE COURT: The defense has rested its case, and the government is presenting one witness in rebuttal.

Agent Ho, do you want to come forward, please? And, sir, you're still under oath from before. When Victoria swears you in, it lasts the whole trial.

WAYMON HO,
having been previously sworn, testified as follows:

DIRECT REBUTTAL EXAMINATION

BY MS. MANCA:

Q. Hello, again, Mr. Ho. I wanted to ask you about some demonstratives that were used in Dr. Halderman's testimony. Were you present for his testimony today?

A. I was, yes.

Q. I'm going to show you Defense Exhibit 1204. Do you recognize this as the demonstrative?

A. I do.

Q. Do you agree with this demonstrative as a depiction of Ms. Thompson's conduct?

A. No. There's a -- it's an oversimplification, and it's missing quite a bit of critical steps.

Q. Can you describe those critical steps for us?

A. Yes.

So in the beginning parts of this, and, you know, from my

prior testimony as well, it's missing the steps where the, you know, the external user, the laptop that's shown on this exhibit, had already scanned and identified a vulnerability within a proxy server.

This is where they would have to already identify what's exploitable, exploit that for the next step in order to attain the -- and you can see it in this exhibit -- the ISRM-WAF-Role. So there is two steps that need to have occurred before this step even happens. It's to, one, identify the step where you can exploit a vulnerable server, and, two, ask it for information about the name of the role. And here, once you have the name, you can request information from the WAF or the credentials.

I'd also like to note that this is the type of request that was shown before, the type of attack that I call a server-side request forgery attack. This is making a web application firewall, which was explained throughout the trial. It's making it do an unintended event. It's making it request an internal resource that is supposed to be protected within Amazon's private network. So it's making it conduct a function that is outside a scope of what the server is intended to do, at least in the cases for the victims that have testified in this case.

Secondly, on the step three here on this exhibit, once that information has been taken from the Instance Metadata Service, the step here that's missing is using another application, the,

you know, the Amazon AWS command line interface, or CLI. It's using -- it's missing that step to use that authentication mechanism to request information.

And then there's more than just "send me data," right? You have to identify the list of buckets that are there. Then you have to sync the buckets. It is also missing, of course, the further part, which is, you know, the copying of data, as well as cryptocurrency mining or deployment.

Q. I'm going to show you Exhibit 1205. Do you recognize that as another demonstrative that was used during Dr. Halderman's testimony?

A. I do.

Q. Do you believe that anything is missing from this demonstrative?

A. Yes.

Q. What is missing?

A. There was no information about the secondary part of the command that was listed at the top, the aws_session.sh. Again, that is another step that is missing from this critical piece, where there is an authentication step. That occurs, too, to gain access to a system.

And if you're looking at the demonstrative at the bottom here, again, yes, you can start a web browser, yes, you can start the settings for a proxy server, and, yes, you can request Instance Metadata Service information once you do that, but,

again, it's missing those same critical steps about, one, how do you know this is the IP address that you can fully exploit that's vulnerable; two, how do you know which name, again, is used to obtain this information; and, three, yes, of course, right, like, the underlying thing is, you know, those beginning parts of steps are required to conduct this function, just like how, yes, if someone had given me, you know, stolen user name and password for Google, yes, I can -- it's easy for me to open up a web browser, go to google.com, and log-in with those credentials, because someone had already given it to me.

So those manual steps are missing that, you know, show the full -- the full scope of the intrusion.

MS. MANCA: Thank you. No further questions.

THE COURT: Mr. Klein, questions for Agent Ho?

REBUTTAL CROSS-EXAMINATION

BY MR. KLEIN:

Q. Mr. Ho, you created the demonstratives yourself, didn't you?

A. Yes.

Q. And they're simplified versions of complex processes, right?

A. Yes.

Q. And these are both demonstratives trying to simplify complex processes for the jury, right?

A. I would assume so.

Q. Yes.

And so with regard to Exhibit 1205, wasn't Professor Halderman's testimony that this was just a simple version of what he would do, and, in fact, he was copying and pasting and putting it in; do you recall hearing that?

A. I guess, yes.

Q. Okay. And then with regard to Exhibit 1204, again, this is meant to simplify a process, but didn't Professor Halderman explain in much greater detail than, actually, this demonstrative of what was happening here?

A. The other pieces were omitted.

Q. Well, they may be omitted from the demonstrative, but I'm asking you, did he talk about this in much greater detail?

A. Than what is displayed on the demonstrative, yes.

MR. KLEIN: One second, Your Honor.

THE COURT: Okay.

MR. KLEIN: Nothing further, Your Honor.

MS. MANCA: I guess, Your Honor...

THE COURT: Okay.

REDIRECT REBUTTAL EXAMINATION

BY MS. MANCA:

Q. To clarify, were aspects of Ms. Thompson's hacking activity that you observed on her device omitted from Dr. Halderman's testimony?

A. Yes, I believe so.

MR. KLEIN: Nothing further, Your Honor.

THE COURT: You may step down, Agent Ho.

All right. So we have finished the testimony in the case, so when you put down your notepads today, Victoria will collect them, and you won't get them back until you're actually deliberating as a jury tomorrow, because I don't want you to put down anything in the notebooks that isn't part of the evidence in the case, testimony or exhibits.

Tomorrow we will instruct the jury. You will each have a copy of the instructions, and I will be reading from the original. The presiding juror will hold on to the original and only write upon the original to fill out the verdict form, but you can write on the copies tomorrow. So you won't have your notepads, but you will have your pens and the ability to write on your instructions, if you want to.

The instruction reading will take about a half an hour, and then the closing arguments will take the rest of the morning, and I imagine we'll submit the case to you right before lunch tomorrow, and then you deliberate until you reach a verdict.

Now, when I used to try cases, the jury would stay into the evening. We don't do that anymore. So we'll be sending you home around 4:00, 4:30, depending on if you want to keep going or you want to leave. Then you would come back Friday at 9:00, and resume your deliberations.

As I said, three of you won't be deliberating in the

afternoon tomorrow, and I'll tell you who you are tomorrow, but it's very important that we don't identify alternates so everyone pays super attention and assumes their part of the deliberating jury.

You've heard all the evidence in terms of the testimony. You haven't seen all the exhibits that have been admitted into evidence. But the most important thing is still ahead are the Court's instructions, which tell you what the law is in this case, and the closing arguments of counsel. So you must still keep an open mind until you hear everything.

So I hope you don't mind going home a little bit early. I promise you, we will keep working to get this ready for you. So tomorrow morning, please be here by ten of 9:00, in Judge Zilly's courtroom, and we'll try to get started promptly at nine o'clock. You are excused for the day.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Thank you. Please be seated.

MR. HAMOUDI: Your Honor, I apologize.

THE COURT: Sure.

MR. HAMOUDI: I didn't want to interrupt the Court as the Court was taking the contract and admitting it. But Mr. Friedman wanted an additional document supplanted to it, and it's a privacy agreement. I don't want that part of the exhibit. I don't think it's relevant.

The only relevance of the agreement that I want is to demonstrate to the jury that this is a service agreement, that you're not actually leasing personal property servers from Amazon. That's really the only thing.

But the government wanted the service -- I handed it to the Court's clerk. And so I have two options. If the Court is going to admit the privacy exhibit, I want to withdraw the whole exhibit in its entirety and not put it in, because it's just going to confuse the jury, or I will ask that only the service agreement be admitted.

THE COURT: What is it about the privacy agreement that --

MR. HAMOUDI: I don't know. Just out of respect for him, he said, "I want this to be a part of it." I handed to it to the Court's clerk, and then to have the Court address it afterwards.

THE COURT: Can I see 1207?

MR. FRIEDMAN: Your Honor, to be clear, the two pages we talked about are actually something called the "acceptable use policy," not the privacy agreement, which we don't care about having. So we're just asking for the acceptable use policy to be included, and it's usually an attachment to the contract.

THE COURT: Why would the acceptable use policy freak you out to the point that you don't want the rest of it in?

MR. HAMOUDI: Because what I don't want to happen in closing is for them to say that her conduct was not an acceptable -- she's not party to that agreement.

THE COURT: Right. That's why they won't say that.

MR. HAMOUDI: If they won't say that, then, Your Honor --

THE COURT: You're not going to argue that, are you?

MR. FRIEDMAN: I don't think so.

THE COURT: So let's admit the entire document with the acceptable use policy, because that is the contract and they should see that.

But we're not going to say that -- I would sustain an objection to any argument that Ms. Thompson is guilty of a crime because she violated the acceptable use policy, because that would be silly, and the government doesn't make silly arguments.

MR. FRIEDMAN: We hope not, Your Honor.

THE COURT: No, not so far, at least.

MR. FRIEDMAN: We're not going to make that argument.

THE COURT: All right.

So in terms of talking about instructions, I'm going to throw a few things out, and if you're not ready to talk about them, we can come back at 2:30 or whatever, if you want to rest your head and thoughts and talk about it.

But the defense wants me to take out "money" and just go with "property" in the instructions, about something of value

that you obtained, money or property, and you wanted to take out "money" and just go with "property"?

MR. KLEIN: Yes, Your Honor.

THE COURT: Yeah. Why?

MR. KLEIN: Because this is over property, Your Honor. I don't think they put in evidence about money. So we just want the jury to be focused on what they've alleged and what they plan to prove, or think they're going to prove.

THE COURT: I'm going to leave both "money" and "property" in there.

And then the government, on some of these "ands" and "ors" and "attempts," what do you want the jury instructed on, on attempt at all or not at all, and then on the "and" and "or," could you go over that, Ms. Culbertson?

MS. CULBERTSON: Sure, Your Honor.

For "attempt," we did not charge attempt in the second superseding indictment as to the wire fraud. So that's why we're suggesting it be taken out.

THE COURT: You don't want "attempt" in wire fraud?

MS. CULBERTSON: Correct. We do want it in Count 9, the access device charge, because it is charged there. And so we believe that's where it belongs, but not --

THE COURT: Only in Count 9?

MS. CULBERTSON: Correct.

And then as to the "ands" and "ors," we have double-checked

them. You charged in the conjunctive, and then instructed in the disjunctive here.

THE COURT: You can instruct in the disjunctive, and that's the way you want it.

MS. CULBERTSON: Yes, that's the way we want it, correct.

THE COURT: And then there's those multiple counts that have -- you know, if you're on the Internet, it's interstate commerce. Rather than repeat that over and over, would you be okay with an instruction that just said, you know, for all of the accounts, "if you're on the Internet, it's interstate commerce"?

MS. CULBERTSON: Absolutely. Whatever your preference is there, Your Honor.

THE COURT: Mr. Klein?

MR. KLEIN: We're fine with that, Your Honor. We have a few other points to raise. I don't want to wait until we come back.

THE COURT: No, no. Go ahead and raise them now, sure.

MR. KLEIN: Your Honor, we had one modification we would propose to the wire fraud instruction, and it's based on commentary in the model Ninth Circuit wire fraud instructions, and I have a copy I can bring up.

THE COURT: Yeah. Just give it to Laura, okay?

MR. KLEIN: And a copy for the government.

THE COURT: Sure.

MR. KLEIN: Your Honor, it's the...

THE COURT: So this is kind of the same issue that Mr. Hamoudi raised about the Bridgegate situation. And, you know, I understand that case. There was a Seventh Circuit case after *Kelly* that said, yeah, that case says this, but if the object of the fraud was the way it was in that case, which was getting the employees to do stuff, then that is property.

I think that that applies in this case, so that's why I think I'm going to deny the motions to dismiss at the end of the government's case and at the end of the defense case, because I think there is an argument that the object of the crime here was to obtain things that are property under the law.

And, look, you have a very good argument that Paige Thompson is not guilty, but it's not that she's wrongly charged, in the Court's estimation.

MR. KLEIN: Your Honor, and I don't know if I need to do this now, but since the government did do the rebuttal, we, of course, renew, again, our Rule 29 motion on the second superseding indictment for all counts.

THE COURT: Sure. I will make an explicit finding that the defense did not waive anything procedurally, and I will deny, deny, deny. Okay?

MR. KLEIN: And then we had two other small

suggestions, Your Honor.

THE COURT: Sure.

MR. KLEIN: There are a lot of victim names thrown out here, and we think it would be helpful to have the jury read the victim names, because you're going to go through the indictment, and they're not identified by name.

THE COURT: I'm not going to read the indictment to the jury. Don't read indictments to the jury.

MR. KLEIN: But still to say who they are, because in Count 1, it doesn't identify the names.

THE COURT: I asked Ms. Daugherty to add Capital One as the victim. The other ones all have victims, I think, except for the access-device ones, right?

MR. KLEIN: I'll double-check that, Your Honor.

THE COURT: Okay.

MR. KLEIN: And then the other small suggestion we had, small change was -- from what we filed the other day -- was for the Jury Instruction No. 29 that we submitted, it was an additional instruction, and it deals with an instruction about responsible disclosure.

THE COURT: Yes.

MR. KLEIN: Based on how the testimony has come in, we would suggest a modification to that at the end. We still want this instruction, to be very clear. But at the end, if you go three lines down, it would say, "and there is no legal

requirement for any person to make any type of disclosure." So we would change it to "any type of disclosure."

THE COURT: Yeah, I'm not inclined to give that instruction at all on responsible disclosure. No one has claimed that Ms. Thompson was under any obligation to make responsible disclosure, and all the witnesses, experts have said it's a process that some companies do, some don't, some are easy, some are hard, but no one said it was a legal requirement, so I'm not going to instruct in that area.

But, of course, the government should not imply that she was under any obligation -- legal obligation to do responsible disclosure. They're free to say that note was not responsible disclosure, and you're free to say, as your expert did, if Capital One had its heads-up, it would have determined that for sure.

Yeah, so Ms. Daugherty just reminded me that I had her add the victim for Count 2, Capital One. And Count 1 is actually a collection of victims, so each one is not going to be mentioned there.

MR. KLEIN: Because we had called that "alleged victim," and that wasn't clear. So thank you, Your Honor, for clearing that up.

THE COURT: We'll give you another set to respond to, so you're not foreclosed here. But have we gone over the ones you wanted to raise for now?

MR. KLEIN: Those are the additional things from what we've submitted, Your Honor, yes.

THE COURT: And then, Ms. Culbertson, do you have any you want to flag for me?

MS. CULBERTSON: No additions to ours --

THE COURT: The ones you sent last night.

MS. CULBERTSON: We do have some thoughts about the ones submitted by the defense. Would you like to hear those now?

THE COURT: No. Wait to see if I give them.

So let's reconvene at 2:30 for you to get a fresh set to look at, not for the court reporter. Just come back. Laura will have copies, two for each side, of my tentative Court's instructions.

MR. KLEIN: Yes, Your Honor. I assume at some point you'll let us formally submit our instructions, if we have disagreement with Your Honor?

THE COURT: Yes. We'll try to do that by four o'clock today, on the record, but I want another round of, "Judge, we respectfully disagree with this, and we respectfully disagree with that, and we don't even respectfully, we just really disagree with this one."

MR. KLEIN: I was told any disagreement is disrespectful.

THE COURT: So give us about 25 minutes to produce a

new set and a verdict form, and we'll get that to you.

We'll be adjourned.

(Court in recess 2:04 p.m. to 3:10 p.m.)

THE COURT: Okay. So we're working from a draft June 15, 2:30 p.m., Court's instructions to the jury, which includes a jury verdict form and 32 proposed instructions. Again, this is informal, but more informal, Ms. Culbertson, do you want to point anything out to us? Not formal exceptions, but is there something that doesn't work?

MS. CULBERTSON: Your Honor, the only suggestion we have is as to Instruction No. 18, so that's for Count 2.

The card issuer -- the financial record of a card issuer is an element the government has to prove, so rather than referring, under the second element, to "information contained in a financial record of Capital One," we think it should say, "in a financial record of a card issuer," and we should include the definition of "card issuer," that's cross-referenced from 1030, back on this page.

As to the identifying that the count relates to Capital One, our suggestion would be to, at the top, "information of Capital One in violation of 1030A(2)" but still keep the reference to card issuer under the second element.

THE COURT: Okay. So let me make sure I understand you.

On line 3, it would say, "information of Capital One,"

comma, "a card issuer."

MS. CULBERTSON: We could do that, or it could just say "information of Capital One."

THE COURT: Okay. And then down below --

MS. CULBERTSON: At line 9.

THE COURT: It would say "information contained in a card issuer"?

MS. CULBERTSON: "In a financial record of a card issuer."

THE COURT: And then a definition of card issuer?

MS. CULBERTSON: Correct. And that's the definition that comes from 15 U.S.C. 1602 that's cross-referenced in 1030(a)(2).

THE COURT: All right. I'll take a look at that.

Did you have a comment about that, at all, Mr. Klein?

MR. KLEIN: I think that's fine, Your Honor.

THE COURT: All right. Let's add that.

And then, Mr. Klein, other things from defense perspective that jumped out at you?

MR. KLEIN: Always, Your Honor.

Well, may we start with the verdict form? Or do you want to do the jury instructions first?

THE COURT: Either one.

MR. KLEIN: It's still the concern we have, in terms of -- if you turn to page 18 for Count 1. It doesn't say who

the alleged victim -- I'm trying to understand. I know you explained it, Your Honor, and maybe I'm missing it. We've been in trial for two weeks, and I'm dense about it.

But I don't see the name of the alleged victim here. And on the verdict form -- the reason why I brought it up -- because it's not clear there, whereas in other places, the alleged victim is listed in parens, and I think it would be helpful to the jury to know who the alleged victims of the wire fraud are supposed to be, because, if I were them, I would be wondering that.

THE COURT: Okay. So that's the main concern is Instruction No. 17 and how it's not clarified on the verdict form either?

MR. KLEIN: I have a couple other concerns, too.

THE COURT: Go ahead. Do them all.

MR. KLEIN: And it's the same -- I'll do it because it is a related concern with Count 8. Again, it doesn't say who the alleged victim is. And that's also in the verdict form, Your Honor, it doesn't say that. So I think there could be clarity there for them, for the jury.

THE COURT: That's Instruction No. 23 you're talking about?

MR. KLEIN: Yes, Instruction No. 23 of the current version -- of the Court's current version, and then it's also page 2 of the current version of the verdict form.

THE COURT: Okay.

MR. KLEIN: And my understanding is that's the alleged Victims 7 and 8 for Count 8.

THE COURT: And another one?

MR. KLEIN: Yes.

Your Honor, just going through these, we stand by our previous issue, some of these previous things.

So the without authorization instruction, which has been modified, we did like Your Honor's original instruction with the one change we made. Instead of saying "public" to say "member of the public." We think that clarity is important.

This instruction, which I understand is drawn partially -- or taking in mind *hiQ*, to be very clear, I understand that, but in *hiQ*, there is no mention of credential requirement or other authentication system, and that's the first subpart. And then in the second subpart, there is no mention of regarding access permissions. And so we like Your Honor's original instruction on that point.

Your Honor, I think I might have brought this up before, I want to make sure. If I've already brought it up, I'm not going to repeat myself. Let me see. I don't know if I raised this last time. I apologize if I'm repeating myself.

But for the Court's Instruction No. 25 for Count 9, we had added at the end -- at the very end, where it talks about intent to defraud, we'd added, in our submission, "the government must

prove beyond a reasonable doubt."

THE COURT: Right, yeah, I'm not going to do that.

MR. KLEIN: If I already brought that up, I apologize.

THE COURT: Let me ask Ms. Culbertson to react to no victim in No. 17 and No. 23.

MS. CULBERTSON: So as to No. 17, wire fraud includes "the scheme to defraud," so my only concern was listing a bunch of victims is confusing the issue as to scheme of the defraud.

THE COURT: I'm having a hard time hearing you.

MS. CULBERTSON: My concern is adding to the scheme to defraud, that listing specific victims is going to confuse the jury as to what it means to have a scheme to defraud.

And then as to Count 9 -- I'm sorry -- 8, so that's instruction --

THE COURT: 23?

MS. CULBERTSON: 23.

So it is charged broadly. It mentions Victim 7, Victim 8, as well as the Victim Cloud Company, which we know is AWS. So I don't think just listing 7 and 8, Survox and 42Lines, captures how it was charged and what the evidence at trial has shown.

THE COURT: Okay. Let me think about some of those. Stay here. At 3:30, I'll come out with the Court's instructions to the jury, and you can take formal exceptions. Okay?

MR. KLEIN: Yes, Your Honor.

THE COURT: All right. Great.

(Court in recess 3:18 p.m. to 4:01 p.m.)

THE COURT: Okay. We have now distributed the Court's instructions to the jury, and we're ready for formal exceptions.

Ms. Culbertson, any formal exceptions from the United States?

MS. CULBERTSON: The United States has no formal exceptions, Your Honor.

THE COURT: All right. Thank you.

And Mr. Klein, for the record, take as much time as you need. From the defense?

MR. KLEIN: Thank you, Your Honor. Hopefully, it won't be too long.

THE COURT: Sure.

MR. KLEIN: Your Honor, I'm going to start with Instruction 17 of the Court's instructions. We continue to believe that the alleged victim should be identified in the instruction. We would continue to believe that the -- and I'll read it out loud -- that the commentary from the model instructions should be added, and, specifically, there should be a conclusion of the concept and the actual -- this language: "Losses that occur as byproducts of a deceitful scheme do not satisfy the statutory requirement."

We would also, with Instruction 17 -- I have to toggle between different things -- when discussing an intent to defraud, the end of that sentence, it should include a sentence

that reads, "the government must prove, beyond a reasonable doubt, that the defendant contemplated some actual harm to the alleged victims' property."

That's it for Instruction 17, Your Honor.

THE COURT: Okay.

MR. KLEIN: Instruction 18 through 22, we object to the definition of "without authorization." So that's for all the instructions that have that definition, we object to it throughout.

THE COURT: Okay.

MR. KLEIN: And we would offer the Court's prior instruction that was circulated, I believe, earlier today. I'll read it out loud.

THE COURT: Okay.

MR. KLEIN: With a modification.

THE COURT: Nice and slow.

MR. KLEIN: I'll go very slow.

"A person accesses a computer, quote, without authorization, end quote, when, one, the computer is password protected or otherwise prevents a member of the public from viewing the information, and, two, the person circumvents the computer's generally applicable rules regarding access permission to gain access to the computer."

That's the definition we believe should be used when instructing the jury.

THE COURT: Okay.

MR. KLEIN: Instruction No. 23 of the Court's instructions, similar to Instruction 17, we believe the victim -- alleged victims should be identified here, Victims 7 and 8. They're not.

For Instruction 25, which is the Court's instruction, which is Count 9, again, with the intent to defraud language, we believe there should be an additional sentence following that that reads, "The government must prove, beyond a reasonable doubt, that the defendant contemplated some actual harm to the alleged victims' property."

And for the intent to defraud or scheme, a sentence in both this instruction and in Count 1, we would strike "money" and just have it be "property" for both of those.

THE COURT: Understood.

MR. KLEIN: We also have offered two additional instructions that are not included that we believe should be included. So the first -- do you want me to list the instruction number from our submission or just --

THE COURT: Just from your submission, right.

MR. KLEIN: Would be Instruction No. 27 of our submission, and that reads, "You have heard testimony and seen an exhibit regarding various Google web searches. Conducting web searches by itself is not a crime, and it is, indeed, protected by the First Amendment's guarantee of freedom of

speech and expression."

THE COURT: Okay.

MR. KLEIN: We have another additional instruction that we believe should be offered. I wish I could just submit it in writing, Your Honor, but I'll read it. It's long. This is Instruction No. 28 from our submission to the Court.

This is what it says: "You have heard testimony that the defendant made statements. It is for you to decide, one, whether the defendant made the statement, and, two, if so, how much weight to give to it. In making these decisions, you should consider all the evidence about the statement, including the circumstances under which the defendant may have made it. Such evidence should always be considered by you with caution and weighed with care. If you determine that the statement is unreliable or not credible, you may disregard the statement entirely.

"Wire fraud, Count 1, 18 U.S.C., Section 1343, requires the defendant act with a specific intent. The act and the specific intent required are explained in that instruction. The defendant is not guilty of wire fraud, even if she says she was, if she did not have the specific intent required for the crime of wire fraud at the time the crime was perpetrated.

"If you have reasonable doubt about whether the defendant had the specific intent required for wire fraud, you must find her not guilty of wire fraud.

"A violation of the Computer Fraud and Abuse Act, defined as CFAA, Counts 2, 4, 5, 6, 7 and 8, 18 U.S.C., Section 1030 requires that a defendant act without authorization. The act and the lack of authorization are explained in that instruction.

"The defendant is not guilty of a CFAA violation if she said she did and/or she had bad intent if she did not act without authorization.

"If you have a reasonable doubt about whether the defendant lacked authorization, you must find her not guilty of a CFAA violation.

"Access device fraud, Count 9, 18 U.S.C., Section 1029, requires the defendant knowingly possess at least 15 counterfeit and unauthorized access devices at the same time with the intent to defraud. The act and the specific intent required are explained in that instruction.

"The defendant is not guilty of possession of unlawful possession of access devices, even if she says she was, if she did not act knowingly and with intent to defraud at the time the crime was perpetrated.

"If you have reasonable doubt about whether the defendant had the knowledge and/or specific intent required for access device fraud, you must find her not guilty of access device fraud.

"Aggravated identity theft, Count 10, 18 U.S.C., Section 1028A, requires that the defendant knowingly possess a means of

identification of another person, knew it belonged to a real person, and did so during and in relation to wire fraud, Count 1, or access device fraud, Count 9.

"The act and specific intent required are explained in that instruction. The defendant is not guilty of aggravated identity theft, even if she says she was, she did not knowingly and in relation to wire fraud or access device fraud. If you have a reasonable doubt of whether the defendant had knowledge required or acted in relation to wire fraud or access device fraud, you must find her not guilty of aggravated identity theft."

Your Honor, that's the objection.

THE COURT: Okay. Thank you very much. I'm going to hold to the Court's instructions as distributed. And notice, thanks to our courtroom deputy, we added the one about how the jury will be allowed to look at the exhibits electronically.

MR. KLEIN: And we don't object to that, Your Honor.

THE COURT: Great. I appreciate that.

MR. KLEIN: We do have two objections to the verdict form, Your Honor.

THE COURT: Okay. Yes. Failure to name victims in --

MR. KLEIN: Count 1 and Count 8, Your Honor.

THE COURT: All right. We will reconvene tomorrow morning to start at 9:00. It will probably take me about a half an hour to read the instructions.

Do you think you'll be longer than an hour in the opening

closing?

MR. FRIEDMAN: I'm pretty confident not longer than an hour and ten minutes; probably an hour.

THE COURT: I'd rather not break up your argument, if at all possible. So, probably, we'll just have you go. If I take more than a half an hour to read the instructions, maybe I'll take a break right then and there.

And then Mr. Hamoudi, probably about an hour.

MR. KLEIN: Yes. I don't know, Your Honor, but when he hears that Mr. Friedman is going to talk an hour and ten minutes, he'll --

THE COURT: He'll do an hour and 11.

And rebuttal closing, Ms. Manca, if we go into the noon hour to finish, we'll just go into the noon hour to finish.

And we will have pens for the jury, along with copies of the instructions so they can take notes, but it won't be in the same place that the notes where taken for testimony and things like that.

I'm very pleased with how we've moved things along, and I appreciate your cooperation greatly.

I will see you tomorrow morning for instructions and closing argument. Thank you.

(Proceedings adjourned at 4:12 p.m.)

C E R T I F I C A T E

I, Nancy L. Bauer, CCR, RPR, Court Reporter for the United States District Court in the Western District of Washington at Seattle, do hereby certify that I was present in court during the foregoing matter and reported said proceedings stenographically.

I further certify that thereafter, I have caused said stenographic notes to be transcribed under my direction and that the foregoing pages are a true and accurate transcription to the best of my ability.

Dated this 15th day of June 2022.

/S/ Nancy L. Bauer

Nancy L. Bauer, CCR, RPR
Official Court Reporter